



DEVELOPING THE INFORMATION WARFARE DEFENSE: A DISA PERSPECTIVE

**ROBERT L. AYERS
CHIEF, INFOSEC PROGRAM MANAGEMENT OFFICE**

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 04121995	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Developing the Information Warfare Defense: A DISA Perspective		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) DISA		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 71		

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 12/1/96	3. REPORT TYPE AND DATES COVERED Briefing	
4. TITLE AND SUBTITLE Developing the Information Warfare Defense: A DISA Perspective			5. FUNDING NUMBERS	
6. AUTHOR(S) Robert L. Ayers				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This briefing discusses Defense Information Systems Agency's (DISA) assigned DoD Agent IW-D responsibilities. It provides the current facts about the support that DISA currently provides and the sheer size of that support. The central message is there are current threats to the Defense Information Infrastructure (DII) and that DISA is taking action and measures to defend the DII as part of their mission.				
14. SUBJECT TERMS IA			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	



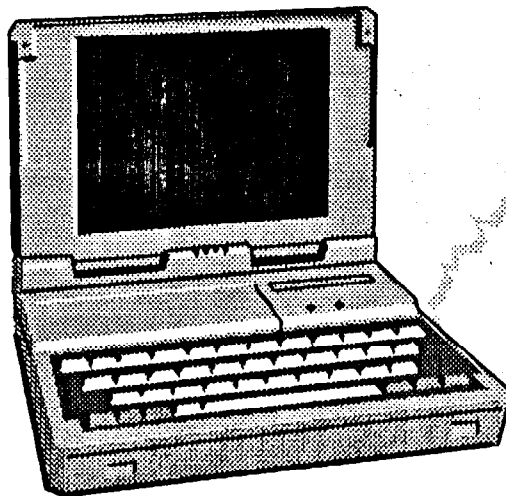
DEVELOPING THE INFORMATION WARFARE DEFENSE: A DISA PERSPECTIVE

**DANIEL T. TWOMEY
IW/INFOSEC PMO
INFOSEC PROGRAM MANAGEMENT OFFICE**



Information , Warfare

Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems...





DISA's IW-D Responsibilities

Director DISA:

will "ensure that DISA Architectures consider EW, ECCM, C3CM"

DODD 3222.4 Electronic Warfare (EW) and
Command, Control, Communications Countermeasures, July 31, 1992

is the "Central Manager" of the DII

DMRD 918, September 1992

will "in consultation with the Directors of the DIA and NSA, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of Defense Information, commensurate with its intended use."

DoDD 8000.1 Defense Information Management Program, October 27, 1992

will "ensure the DII contains adequate protection against attack."

DoDD TS 3600.1, Information Warfare, December 21, 1992

will "assess the vulnerabilities of ... defense information systems" and to "maintain procedures to ensure a capability to respond to identified threats and assessed vulnerabilities

CJCS MOP 30, Command and Control Warfare, 8 March 1993

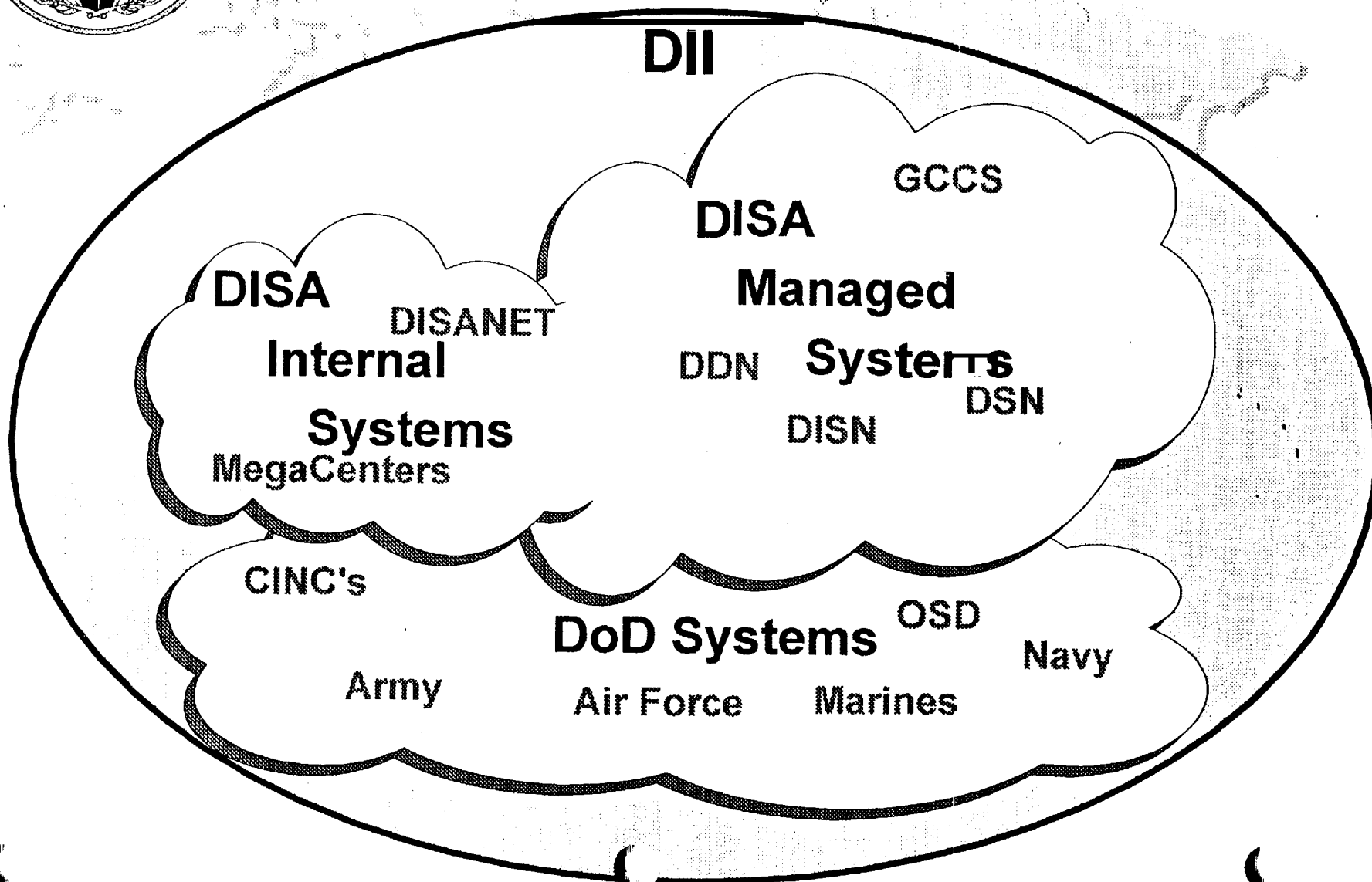


DISA's Assigned DoD Agent IW-D Responsibilities

- **Technical Standards**
- **Training and Courseware**
- **DoD Computer Emergency Response (Also Army)**
- **DoD MLS Program**
- **Goal Security Architecture**
- **Security Architecture and Engineering Support**
- **Standardized Certification and Accreditation Policy**
- **Lead Security Officer Program**
- **DoD Open IW Contract Vehicles**
- **Security Product Requirements and Development**
- **DoD IW-D Management Planning and Management**
- **DII Protection (IW-D Operations)**



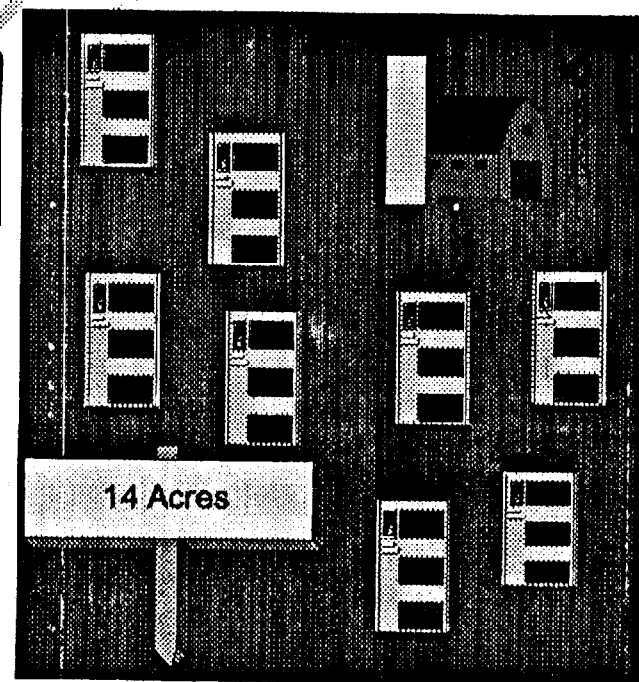
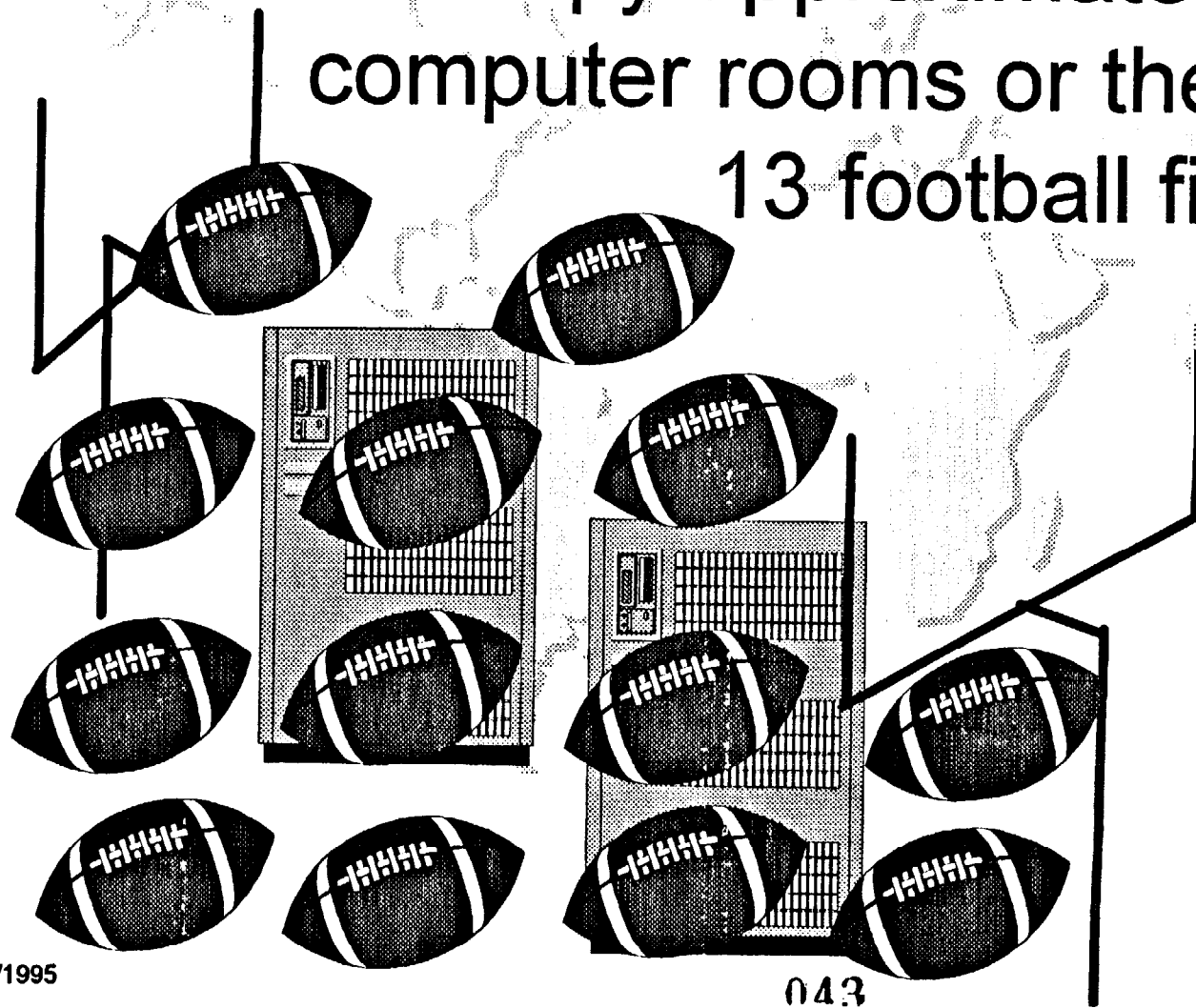
Defense Information Infrastructure





DISA FACTS: MEGACENTER COMPUTERS

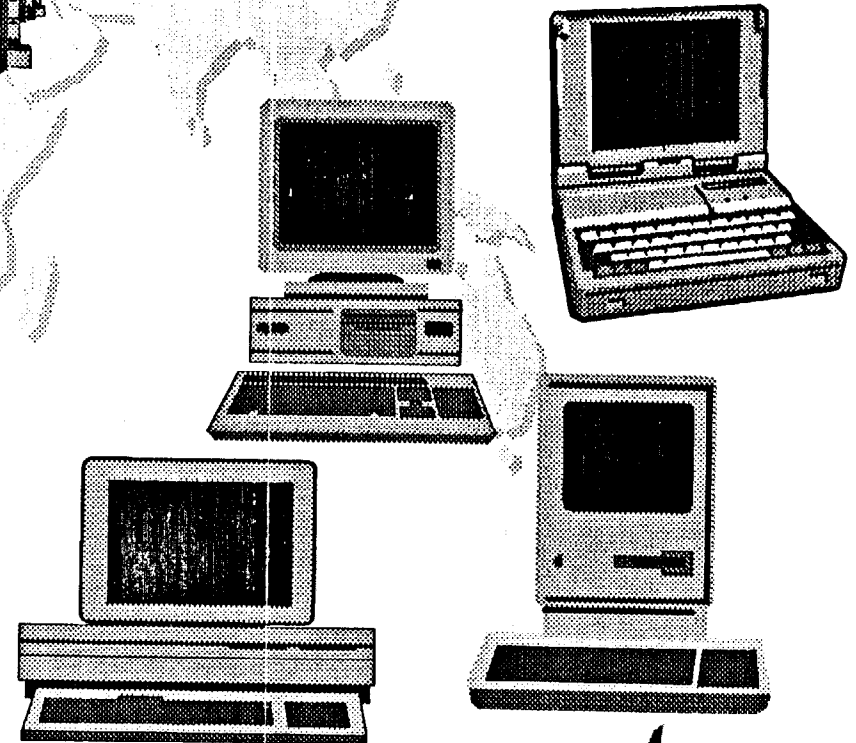
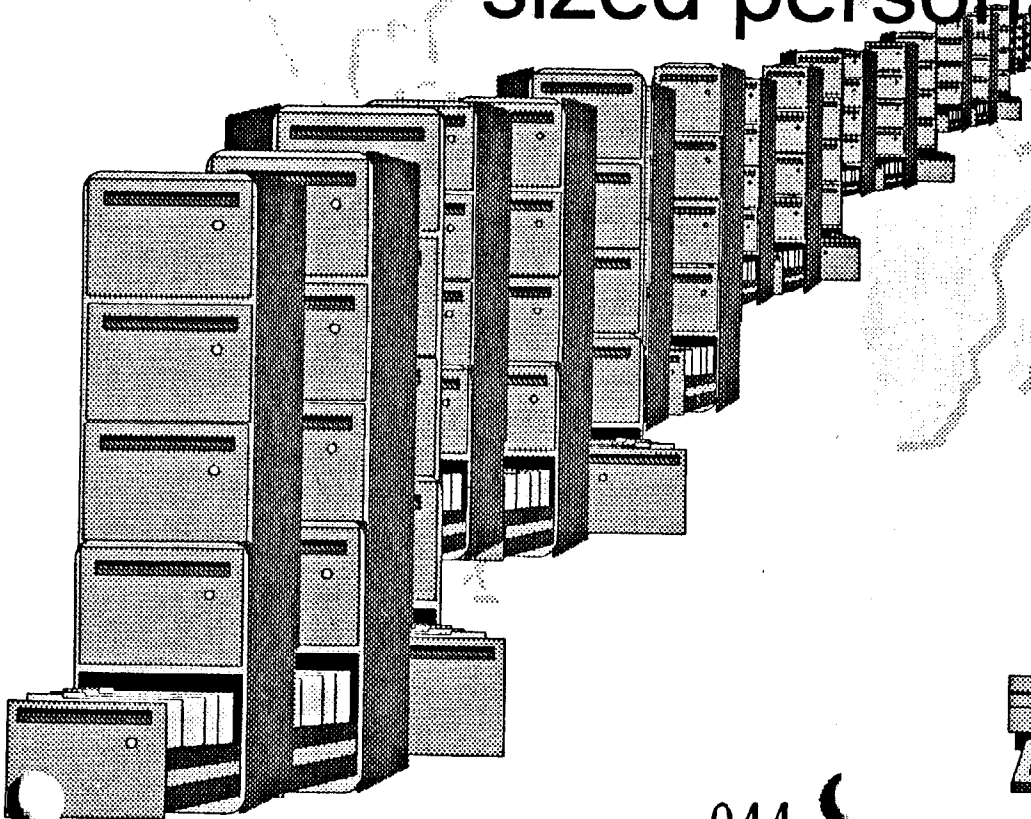
Computers in DISA megacenters occupy approximately 14 acres of computer rooms or the space of over 13 football fields.





DISA FACTS: MEGACENTER DATA

Data in DISA megacenters could fill over 1,000,000 five drawer file cabinets or over 50,000 average sized personal computers.





DISA FACTS: MANAGED SATELLITES

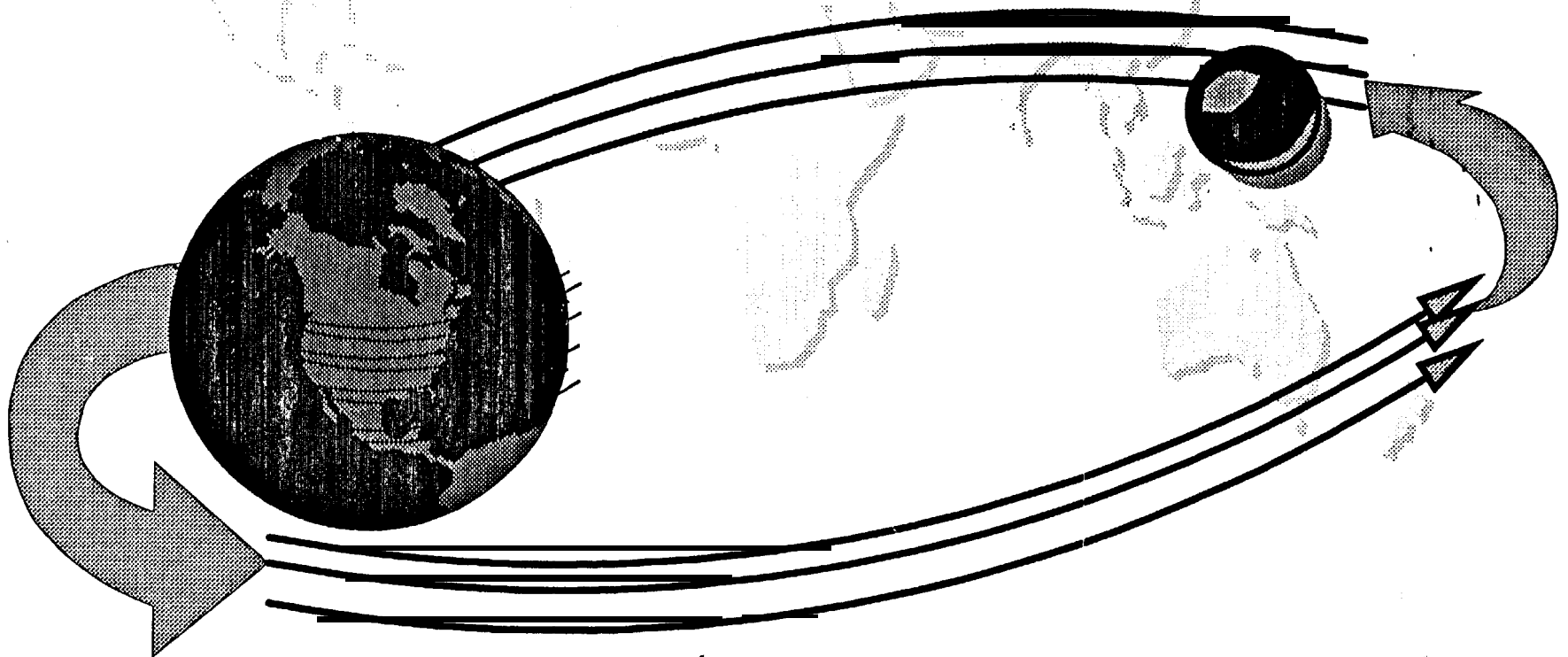
DISA managed
satellites move more
information in a
single day than a
stack of books 681
miles high





DISA FACTS: DIGITAL NETWORKS

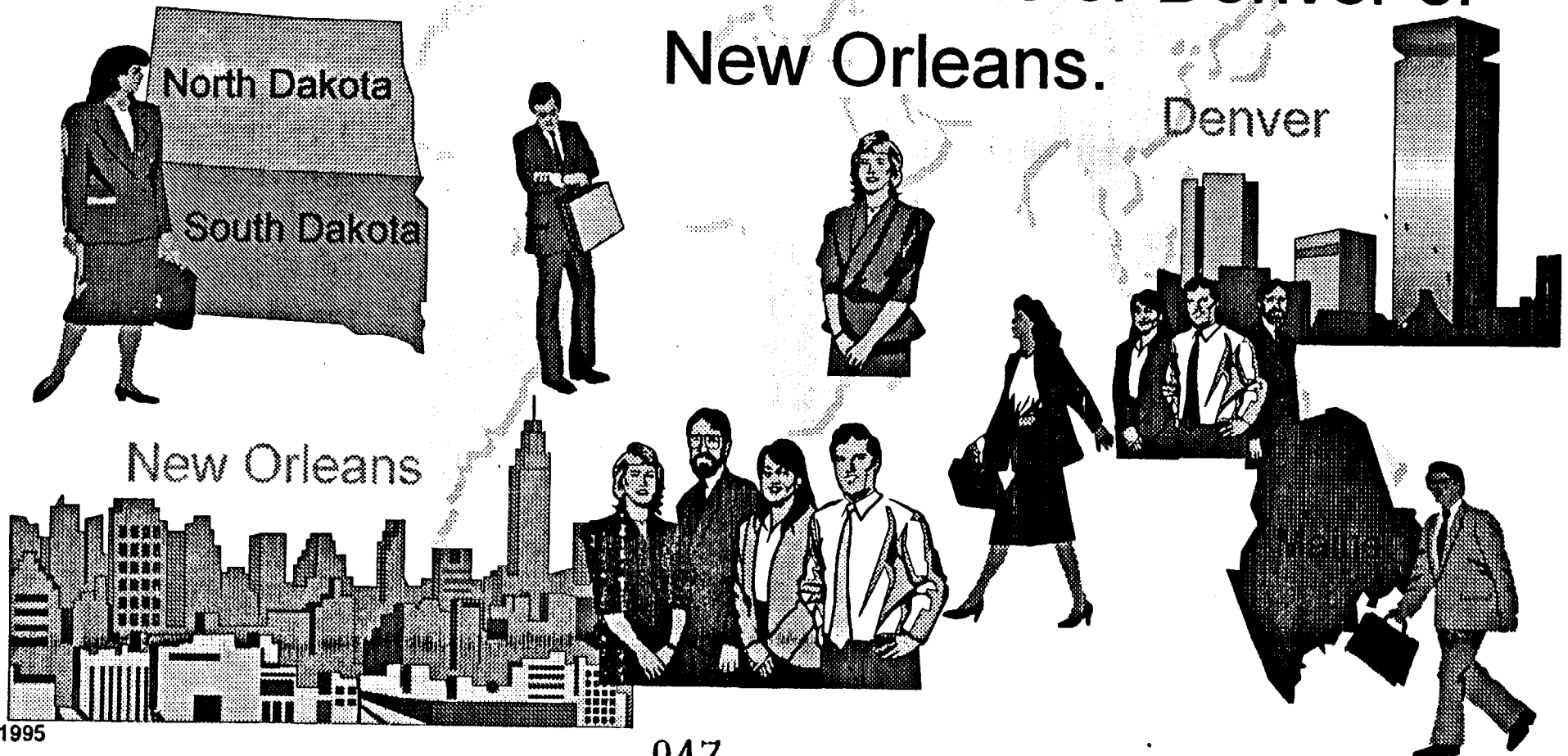
DISA Digital Networks could circle the globe 400 times or go to the moon and back 21 times





DISA FACTS: DEFENSE MESSAGING SYSTEM

DISA's DMS serves more users than
the entire population of North and
South Dakota or Maine or Denver or
New Orleans.





Info Warfare (IW) - Defend

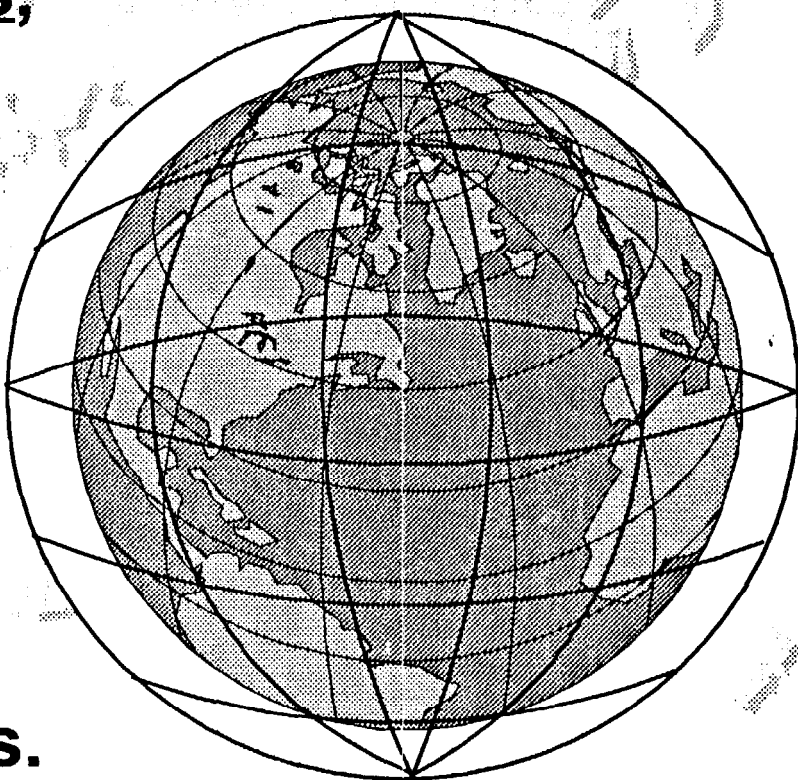
Objective

Assured Information Service



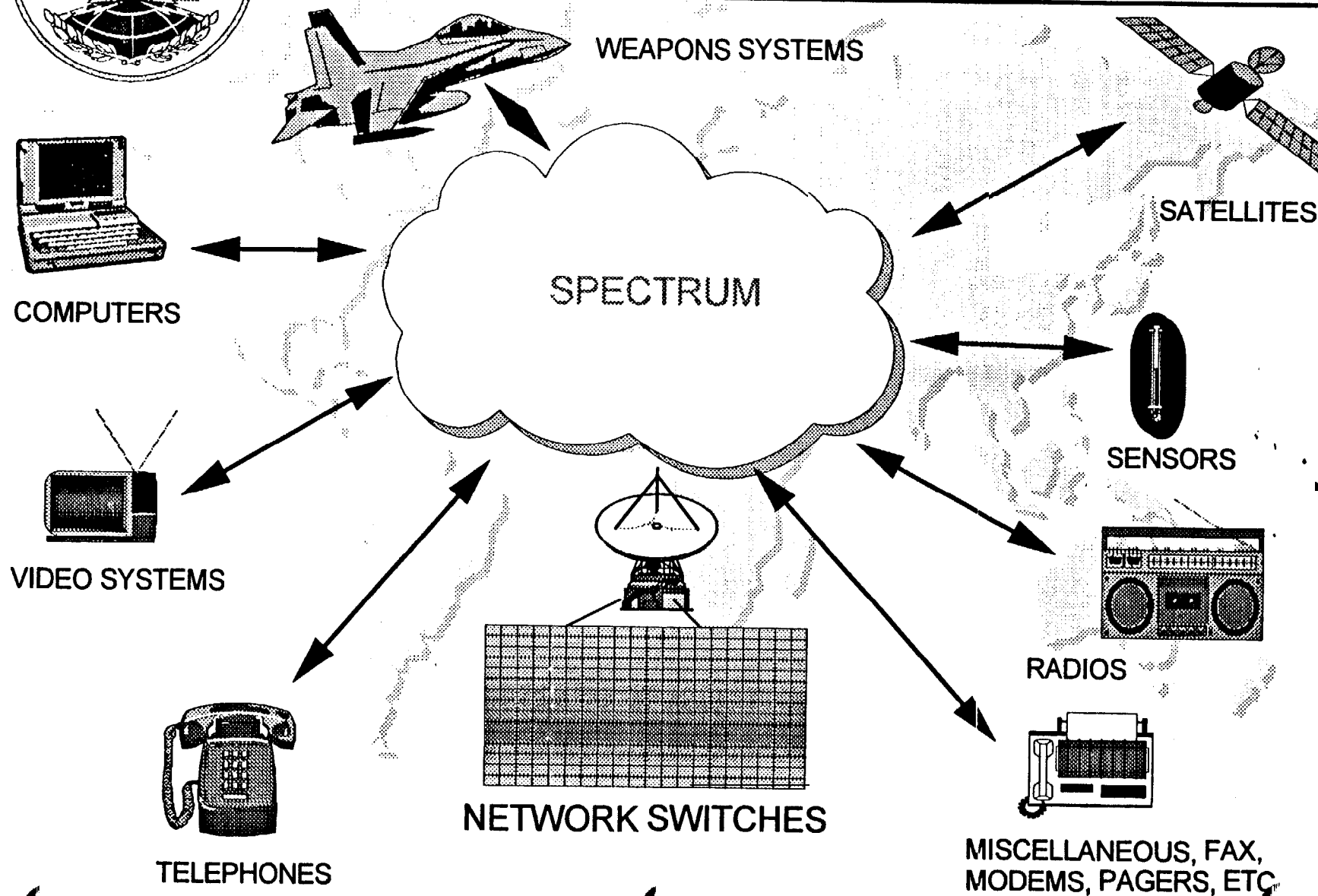
The Defense Information Infrastructure

A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and v&time roles.



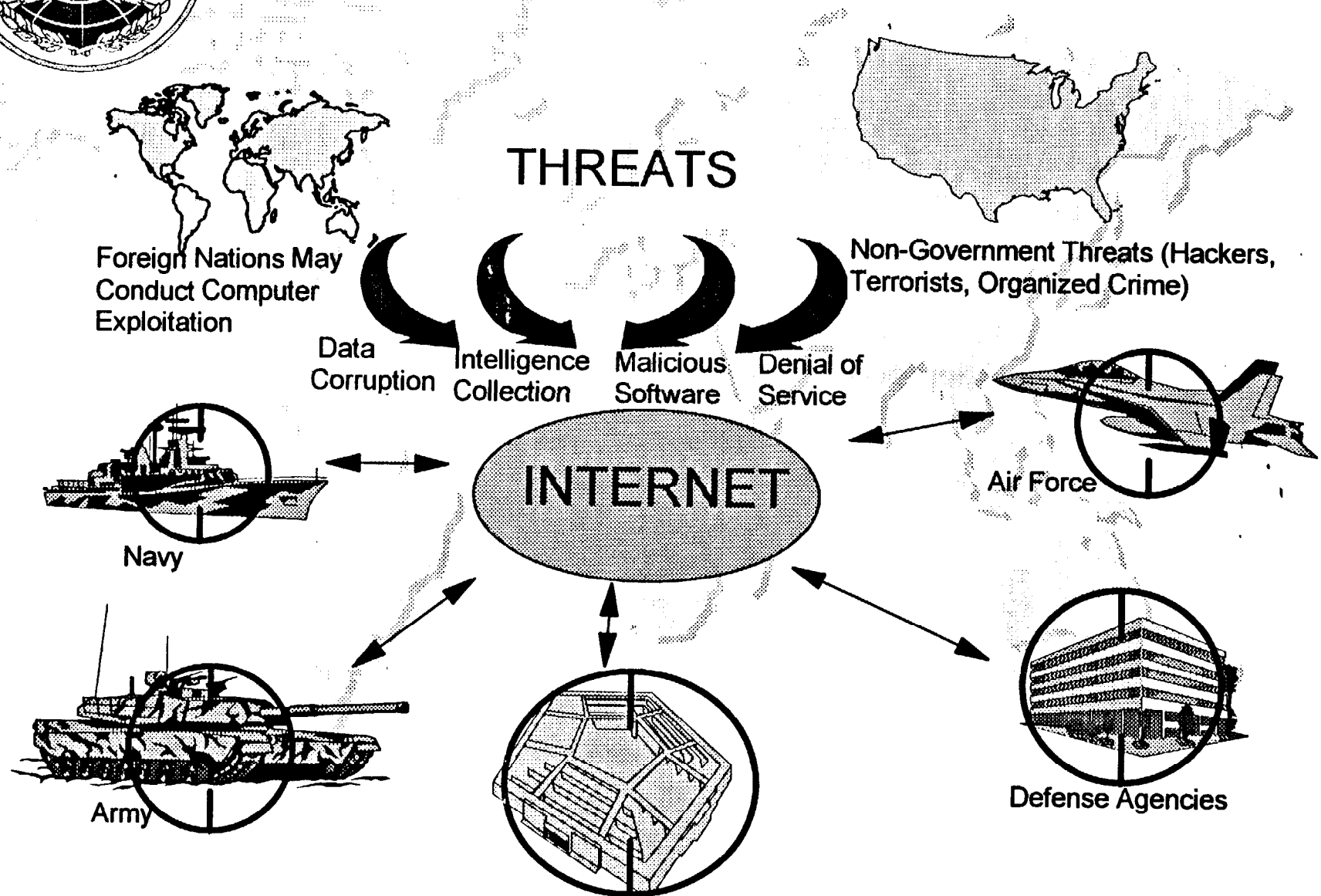


The DII an Infrastructure View





Threats to DoD Networks





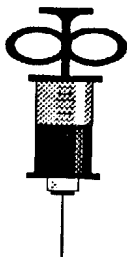
DII Threats



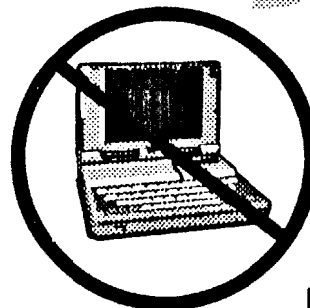
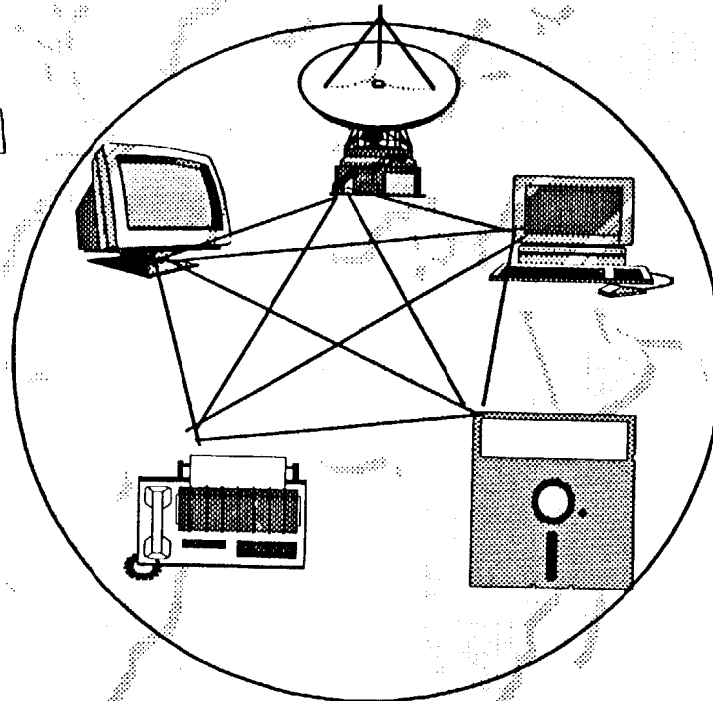
HACKERS



ESPIONAGE



MALICIOUS CODE



DESTRUCTION



THEFT OF SERVICE



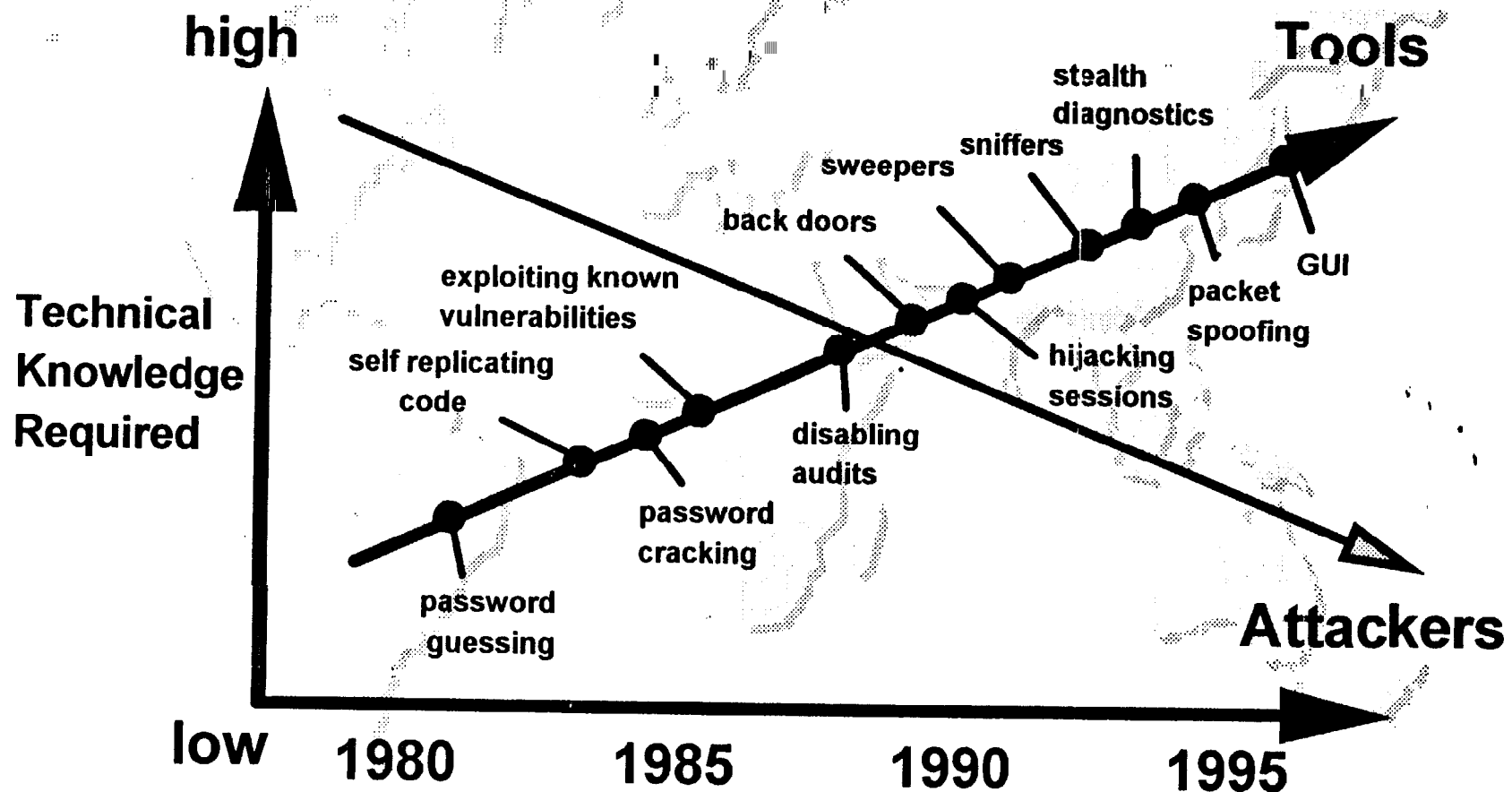
FINANCIAL GAIN



JAMMING



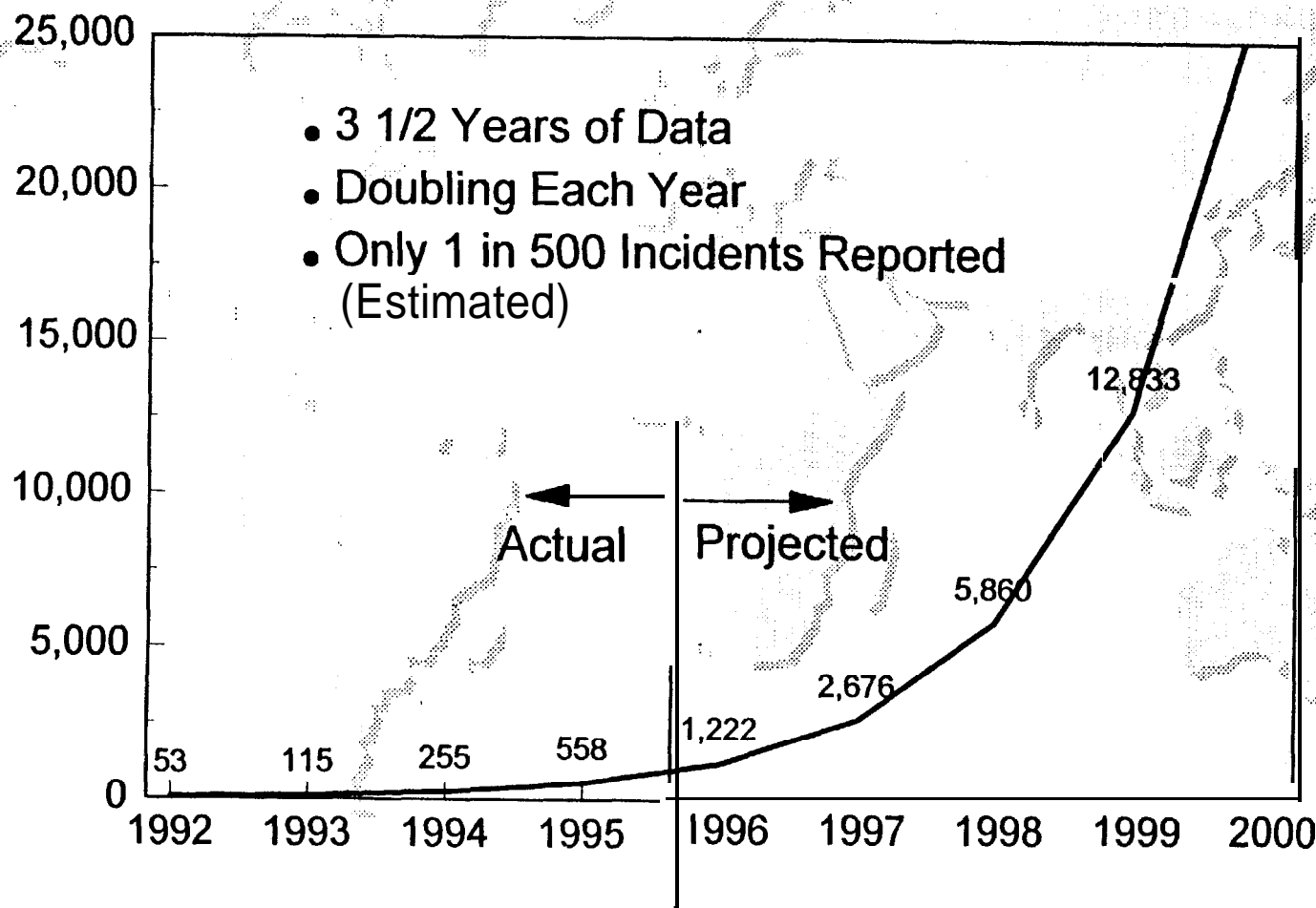
Intruder Technical Knowledge





Reported Security Incidents*

* An incident is any event in which a computer system is attacked, intruded into, or threatened with an attack or intrusion.





Approach To The Threat

Yesterday

Risk

Avoidance

- Tempest Program
- Physical Isolation
- Certified Products

-
- Know your vulnerabilities and operate no system with vulnerabilities

Change

Dynamics

- Shrinking budget
- Worldwide pursuit for universal connectivity
- Consolidating of DOD's information infrastructure
- Increased reliance on Commercial Products
- Increased reliance on Commercial Service Providers

Today

Risk

Management

- Absolute protection is technologically impossible
- Financially impossible to buy absolute protection
- Know your vulnerabilities, operate with them, but manage them



Information Warfare



Defending The DII

The
New
Battleground



DISA IW Mission

**"...AS CENTRAL MANAGER FOR THE DII,
SHALL ENSURE THE DII CONTAINS
ADEQUATE PROTECTION AGAINST ATTACK."**

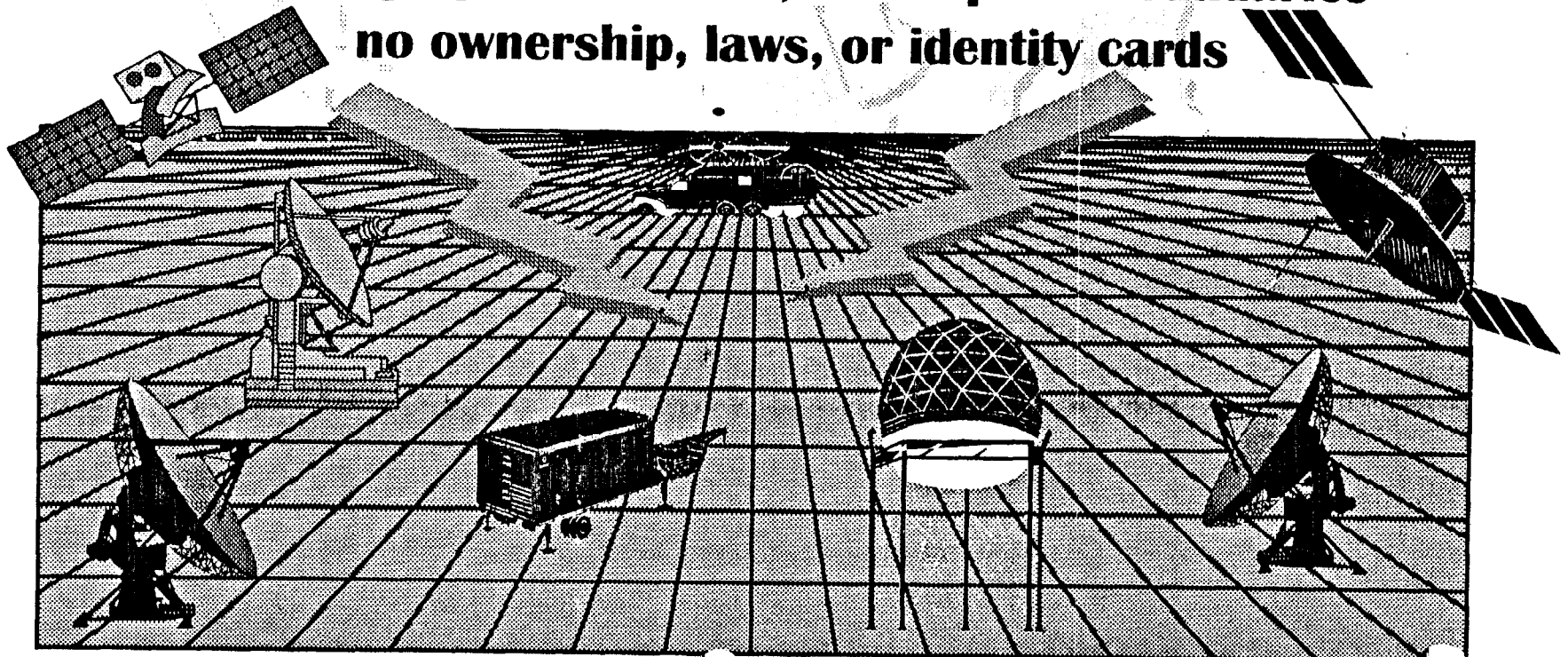
DOD D 3600.1

Information Warfare Cyberspace



The electronic environment formed by the aggregate of global computing and telecommunications resources.

Cyberspace is a virtual 5th dimension characterized by:
no geographic, national, or temporal boundaries
no ownership, laws, or identity cards





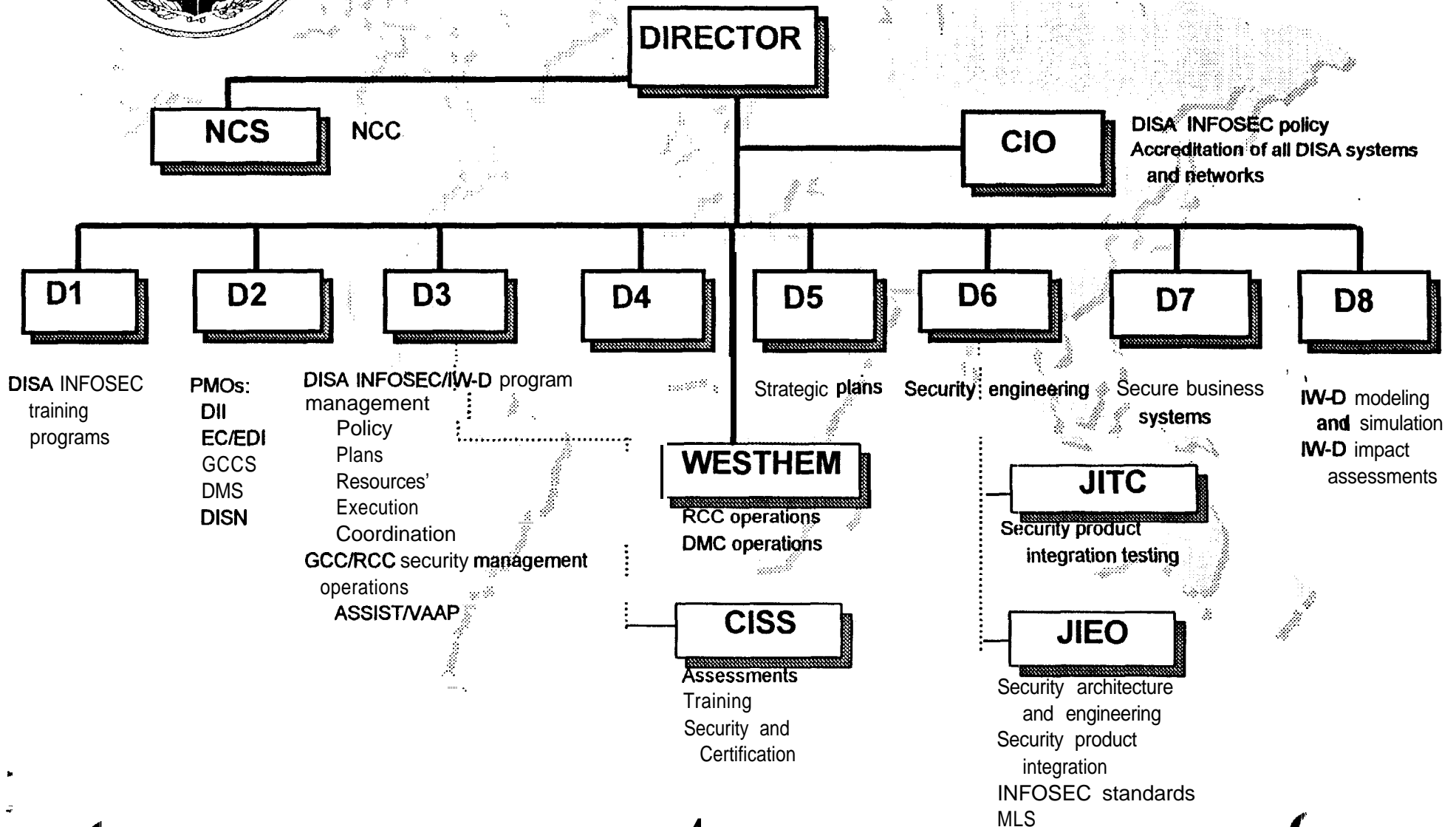
Information Warfare

A New Reality

- **Defense information is a target.**
 - The DII will be the battlefield**
 - **The world knows we are dependent on information for our style of war**
 - **Adversaries already have attack capabilities**
 - **Open literature has examples**
 - **High school students have succeeded**
 - **Low cost/high payoff**
 - **Strategic advantage for low tech armies**



DISA IW-D / INFOSEC FUNCTIONAL RESPONSIBILITIES





Security for the DII provided thru a BALANCE of:

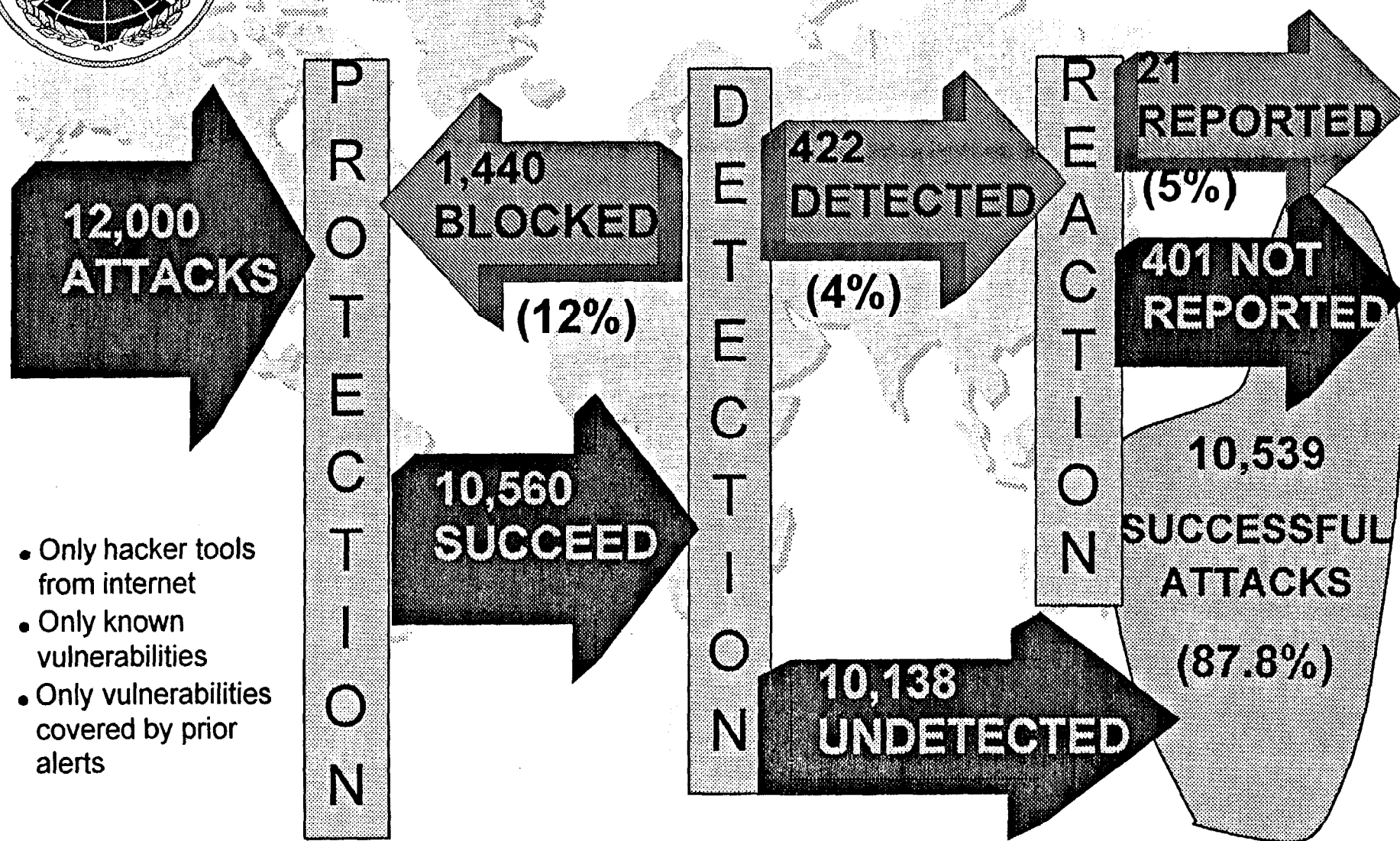
PROTECTION: PROTECT critical DII networks, systems and facilities

DETECTION: DETECT attacks upon the DII quickly enough to enable operational reactions

REACTION: Operationally REACT to attacks to either defeat them or maintain service



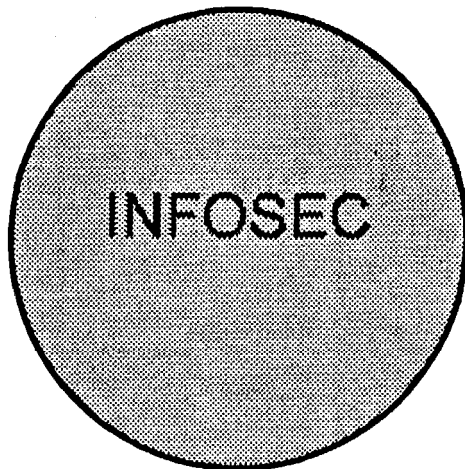
Red Team Assessment of DoD Security Mechanisms





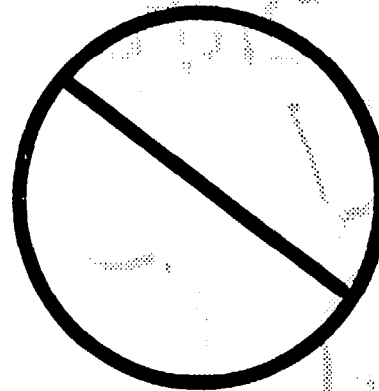
Historical Roles

Protect

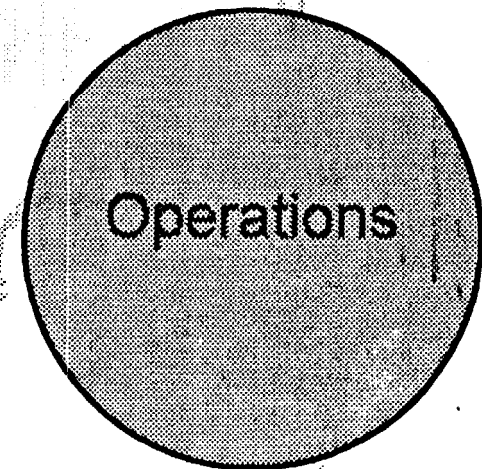


Certification
Encryption
Passwords
System Isolation

Detect



React



Fault Isolation
Repair
Performance Balancing
Backup and Recovery



IW-D is a Unifying Mission

Protect

Detect

React



Risk Management Philosophy for Security of the DII

**Absolute protection of the entire
Defense Information Infrastructure
(DII) is neither technically nor
financially achievable. Some number
of attacks upon the DII will succeed.**



PROTECTION Program

Secure critical backbone communications network (DISN) and connection to it

Secure critical military applications:

Global Command and Control System

Defense Messaging System

Business processes (finance, medical, logistics, personnel)

Secure critical processing centers (Defense Megacenters)

Train and equip system administrators for secure operations



DETECTION Program

Continually measure DII vulnerabilities to attack

Develop and implement attack detection technologies

Train and equip security personnel for attack detection



REACTION Program

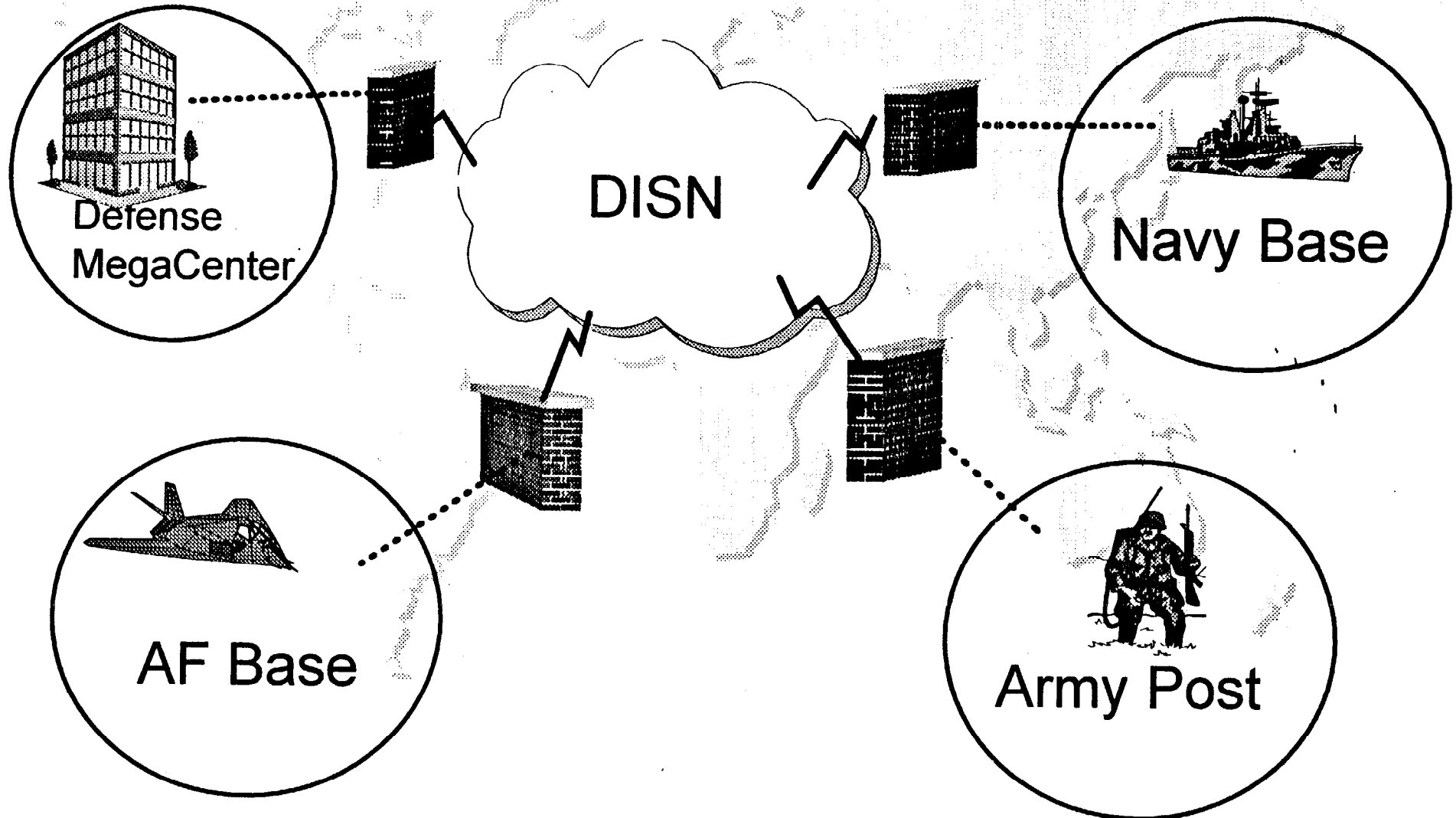
Upgrade DII Global and Regional Control Center System by:

- ▶ Adding attack recognition function
- ▶ Adding automated infrastructure reaction management capability

Train, equip, and exercise Global and Regional Control Center personnel in defensive information warfare

Secure the Network

World 'Wide DISN





Secure the Network Infrastructure/Connectivity

DISN Examples

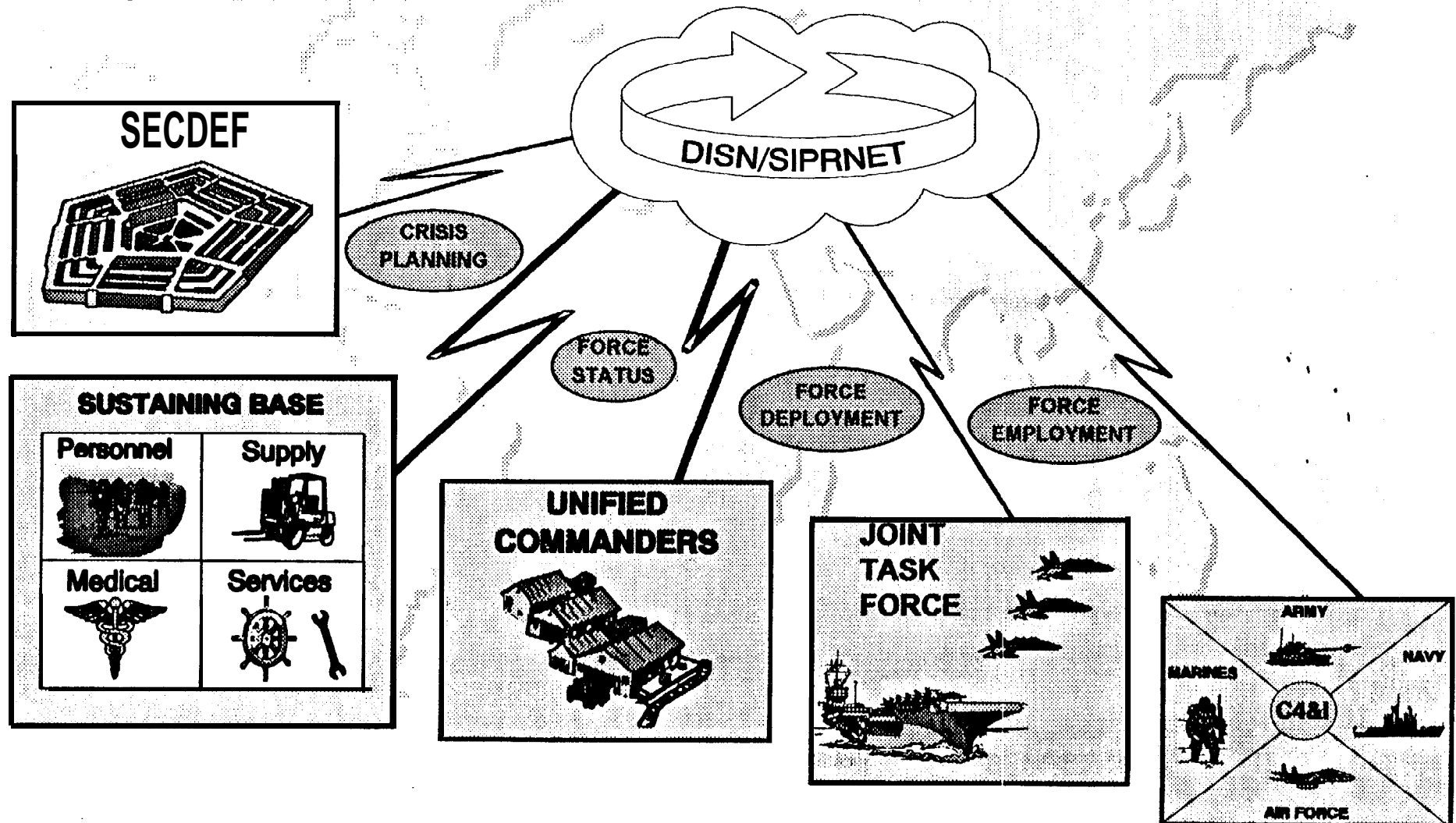
- CONUS/DISN Backbone
- OCONUS Links
- NIPRNET
- SIPRNET
- JWICS Infrastructure

Task Number 2.1	FY96	FY97	FY98	FY99	FY00	FY01
Procure High-Speed Encryptions and Hardware/Software to Secure Network Management Centers	▲					▲
Procure Secure Network Servers (SNS)		▲	▲			▲
DISN Collapses to Single Network					▲	
Procure FORTEZZA Cards and Certification Authority Workstations (CAWs)	▲	▲				
Procure FORTEZZA+ Cards and Certification Authority Workstations (CAWs)		▲	▲			
Procure PCMCIA Card Readers	▲	▲				



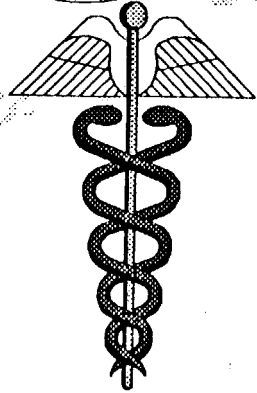
Secure the Applications

Global Command and Control

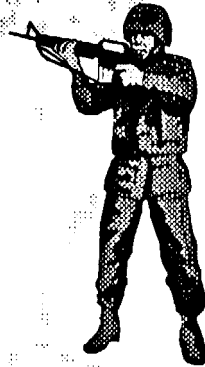




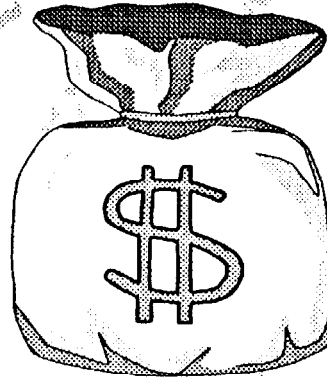
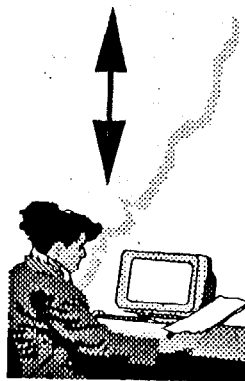
Secure the Applications Business Applications & Users



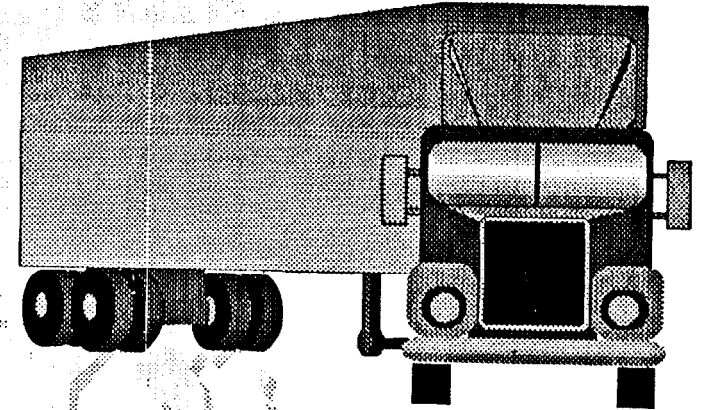
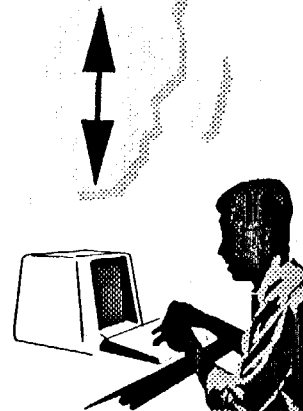
Medical



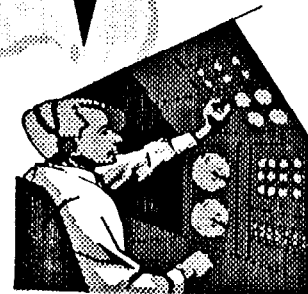
Personnel



Finance



Logistics





Secure the Applications

GCCS Examples

• MLS into GCCS

Task Number 4.1	FY96	FY97	FY98	FY99	FY00	FY01
Procure and Install Multi-Level Security (MLS) Workstations, Trusted Operating Systems and Trusted Servers		▲	▲	▲		
Procure and Install Imagery Guard and GCCS/GCCS-T Guard			▲	▲		
Procure and Install GCCS Intelligence Workstation			▲	▲		
Port GCCS MLS Software to HP Workstations				▲	▲	
O & M for Fielded Systems and Upgrading to New Technology			▲	▲		▲



Secure the Applications

DMS Examples

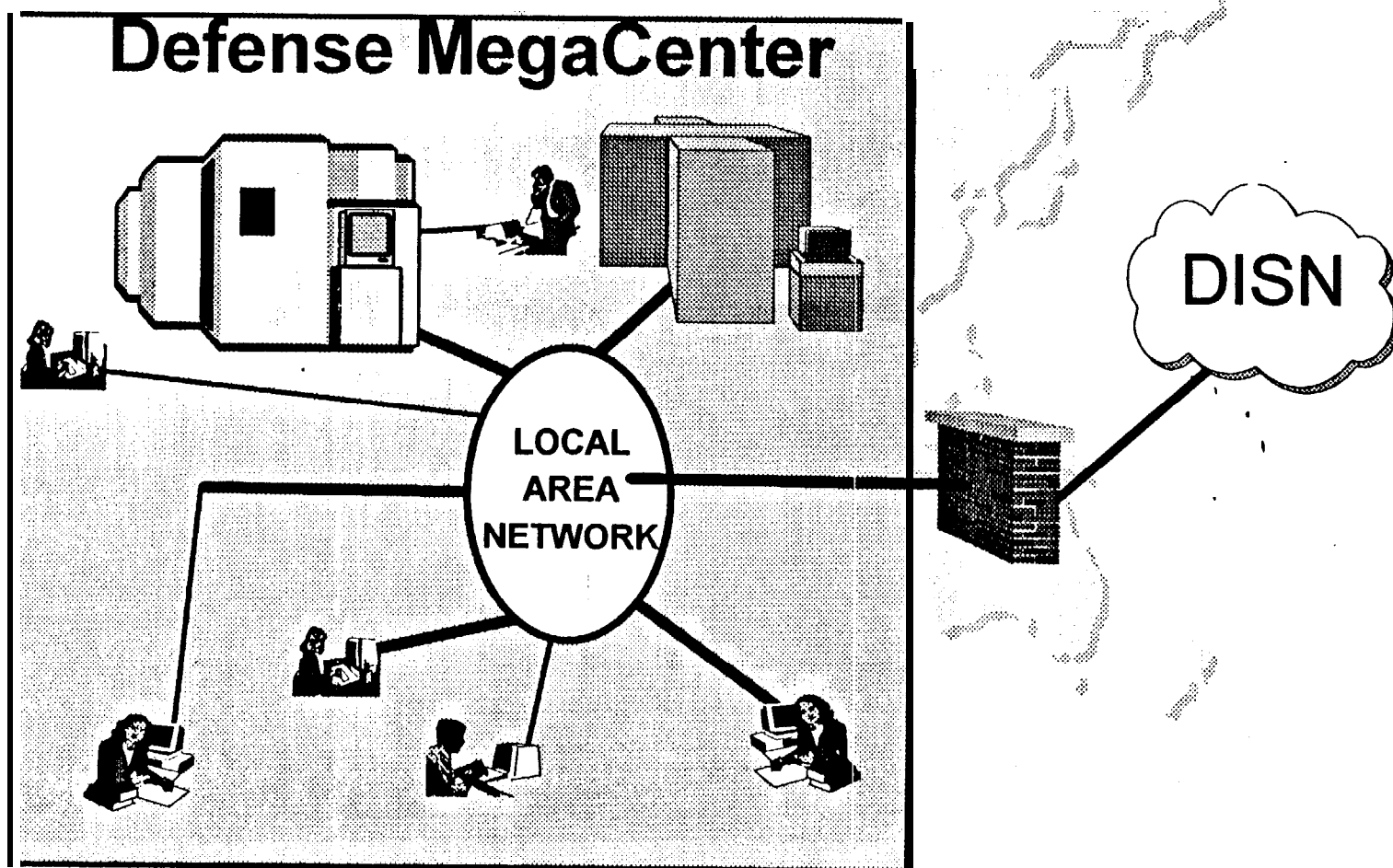
- APIs for Business Systems
- DMS

Task Number 4.3	FY96	FY97	FY98	FY99	FY00	FY01
DMS Implementation (Sensitive but Unclassified)	▲				▲	
DMS Implementation (Unclassified to Secret)		▲			▲	
DMS (Interim Top Secret/SCI)			▲			
Autodin Phase Out					▲	
Full Multi-Level Secure Operations						▲

* The DMS Phasing depicted above is based on the DMS Migration Strategy as of 18 October 1995 and is under control of the DMS PMO. It is provided as a part of this INFOSEC Plan for information purposes. The Joint Staff approves/disapproves shutdown of individual AUTODIN Switching Centers (ASCs) on a yearly basis.



Secure the Defense Megacenters





Secure the Defense Megacenters

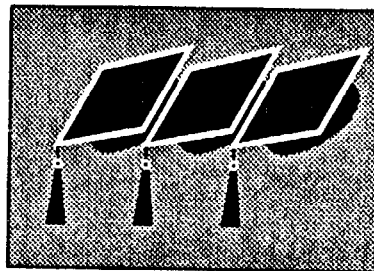
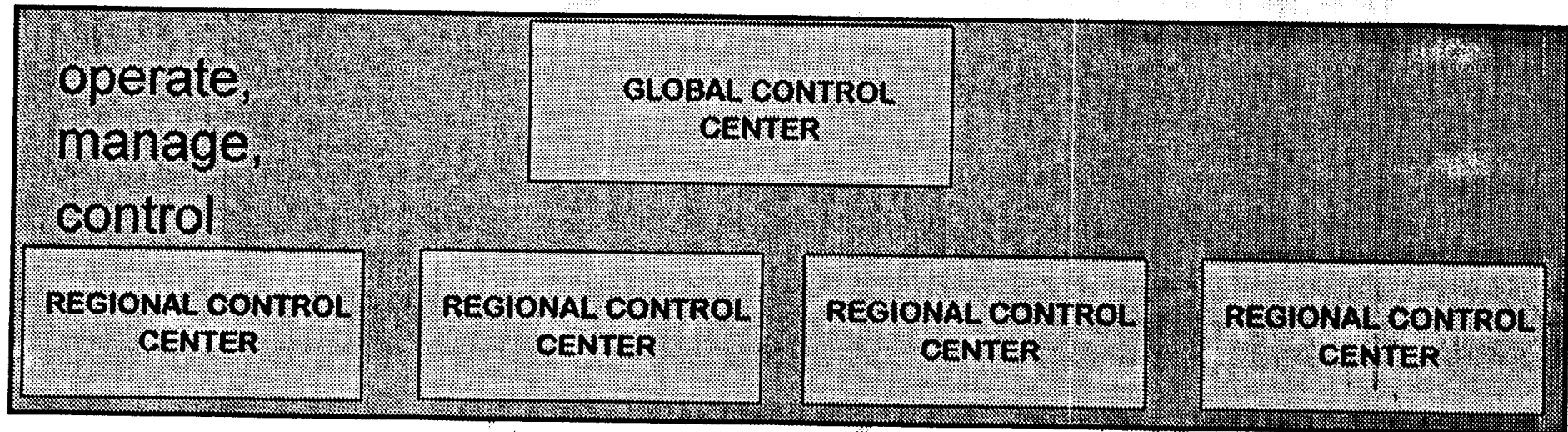
DMCs Examples

- Integrate MISSI Technologies
- Standardize Environment
- Certification
- Vulnerabilities
- Security Deficiencies

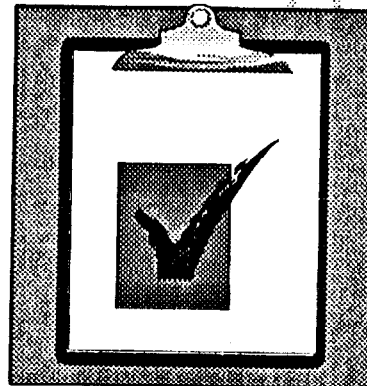
T&k Number 3.1	FY96	FY97	FY98	FY99	FY00	FY01
DMC - Columbus EOP	▲	▲				
MVS Systems	▲			▲		
Unisys Systems		▲		▲		
UNIX systems	▲			▲		
Other Systems		▲				▲
Maintenance	▲	▲	▲	▲	▲	▲



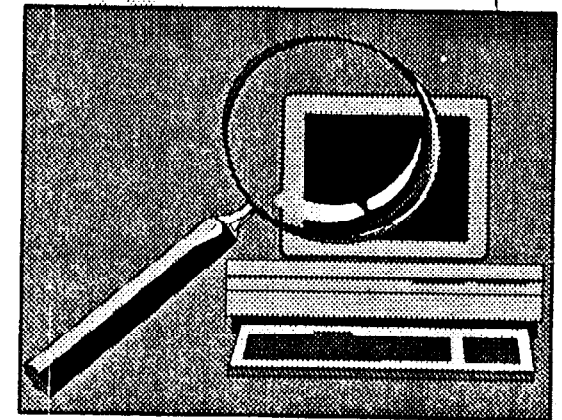
Operate and Manage a Secure DII



Train Personnel



Certification/Accreditation





























**Measure
Vulnerability**



Operate and Manage a Secure DII

Examples

- Certification & Accreditation
- Training
- Red Team
- Security & Ops.
- Mgmt.Integ.

Task Number 53.2	FY96	FY97	FY98	FY99	FY00	FY01
Global C2 System						
Defense Megacenters Certification/Recertification	4 	8 	6 	R-6 	R-6 	R-6 
DISA-EUR				R 		
DISA-PAC					R 	
SIPRNET				R 		
NIPRNET				R 		
DISANet				R 		
Other DISA Systems						
DoD Certification Support (e.g., TACCIMS, EKMS)	 (DISA Funded)			 (User Reimbursable)		



Global Control Center Regional Control Center

Concept



Goal of Global/Regional Control Centers

Significant improvement in military readiness and war fighting capability by:

- ▶ Ensuring availability of information services by preventing or operationally reacting to common information system attacks
- ▶ Ensuring the confidentiality and integrity of all DoD communications and businesses



Strategic Objectives

Assured Information Service to CINCs

Battlespace Management (DISA is Cyberspace Warfighter)

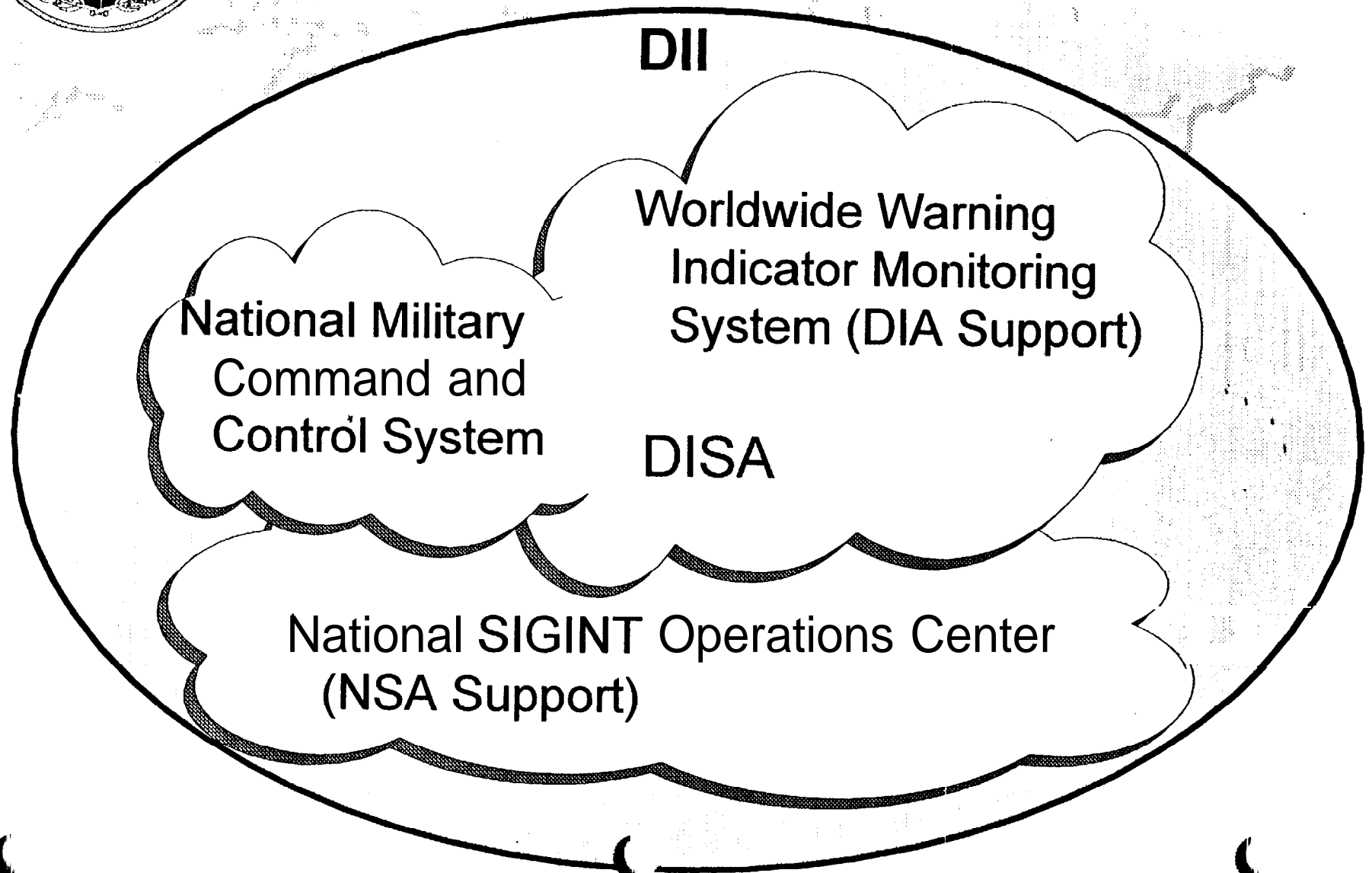
Integration into Worldwide Warning Indicator Monitoring System (DIA Support)

Integration into National Military Command and Control System

Tie to National SIGINT Operations Center (NSA Support)



Center Connections





CONOPS

Proactive detection and reaction

Hierarchical Relations"

Routine vs 'Crisis Operational Modes

Nominal Control Center Model

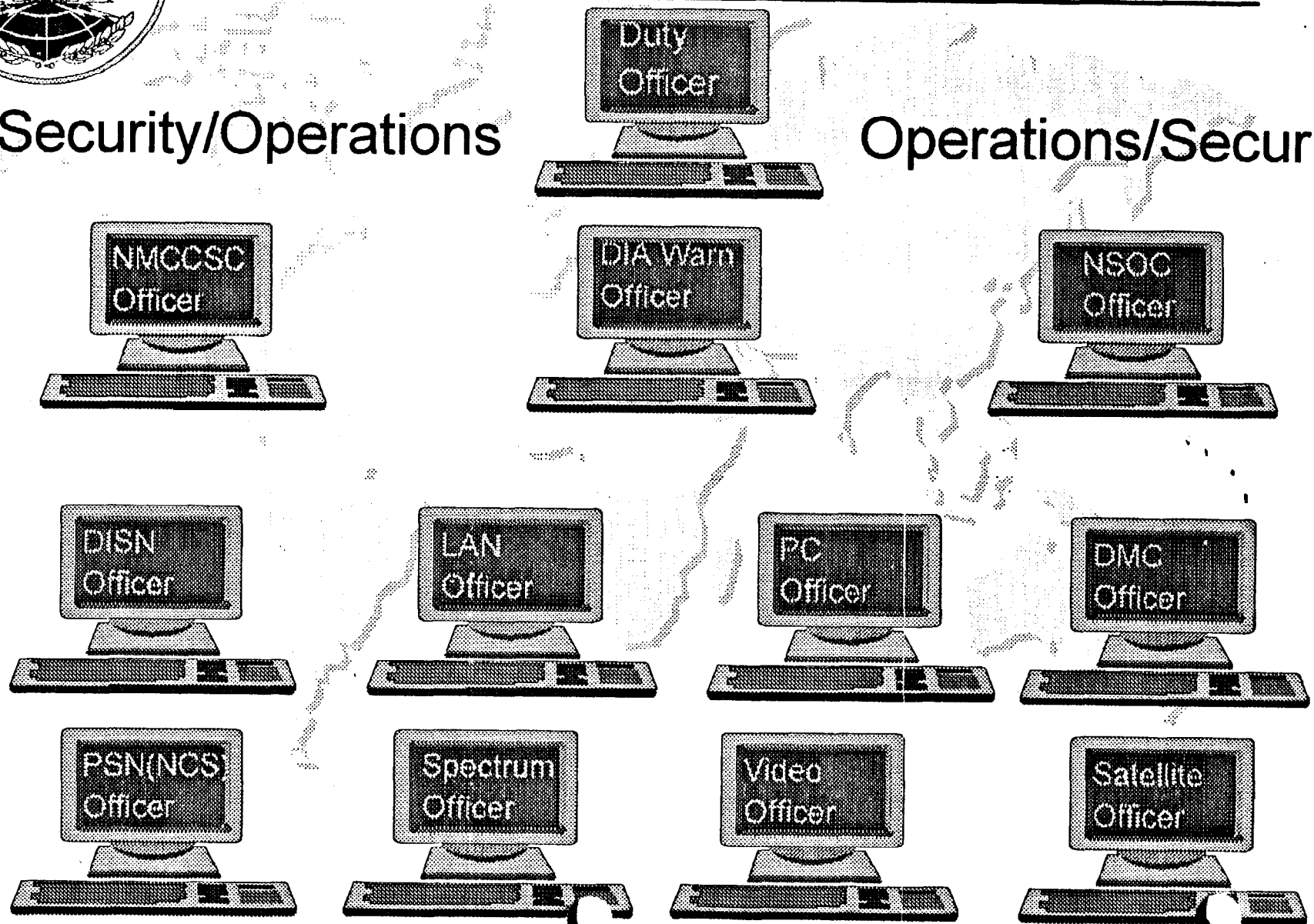


Global/Regional Control Center

A Functional View

Security/Operations

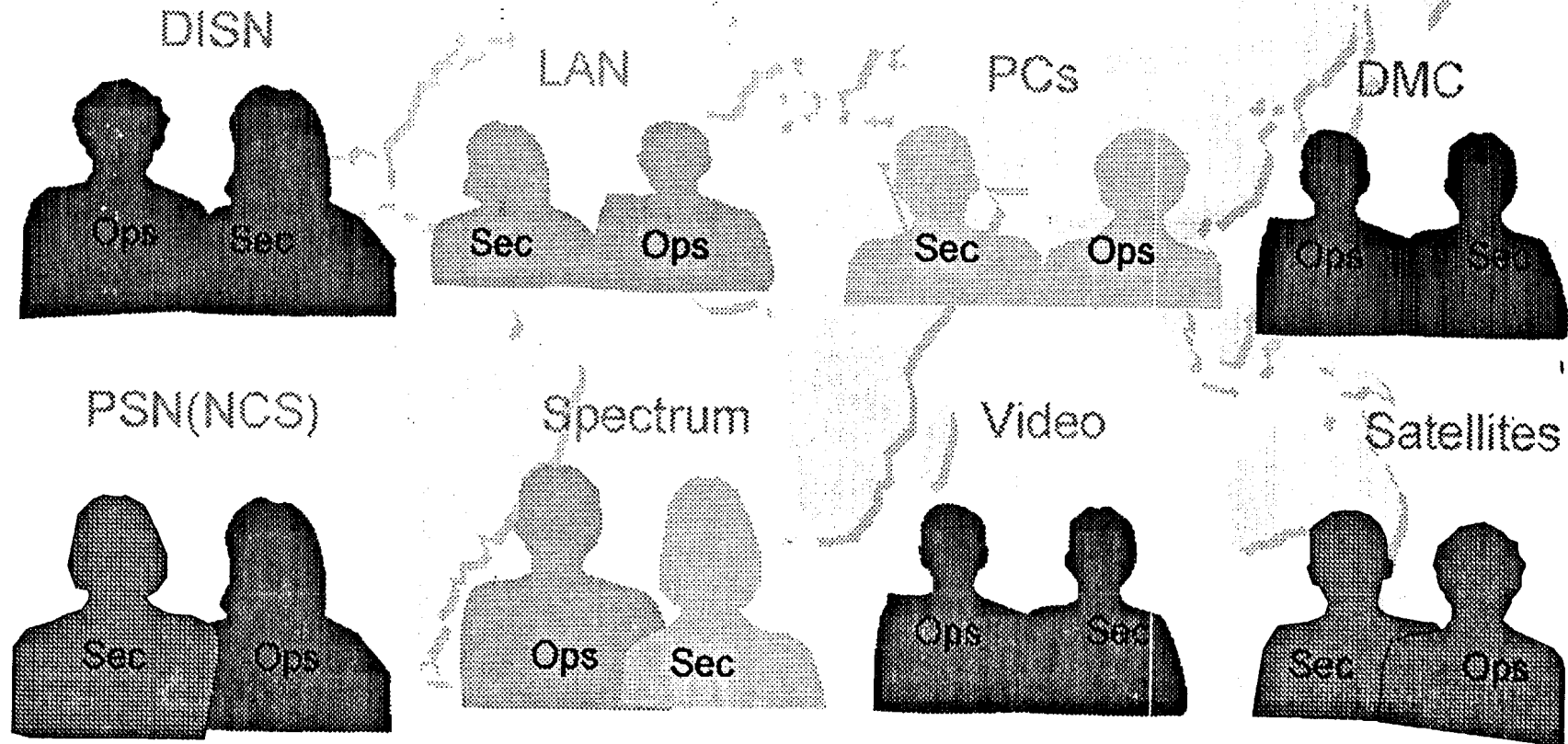
Operations/Security





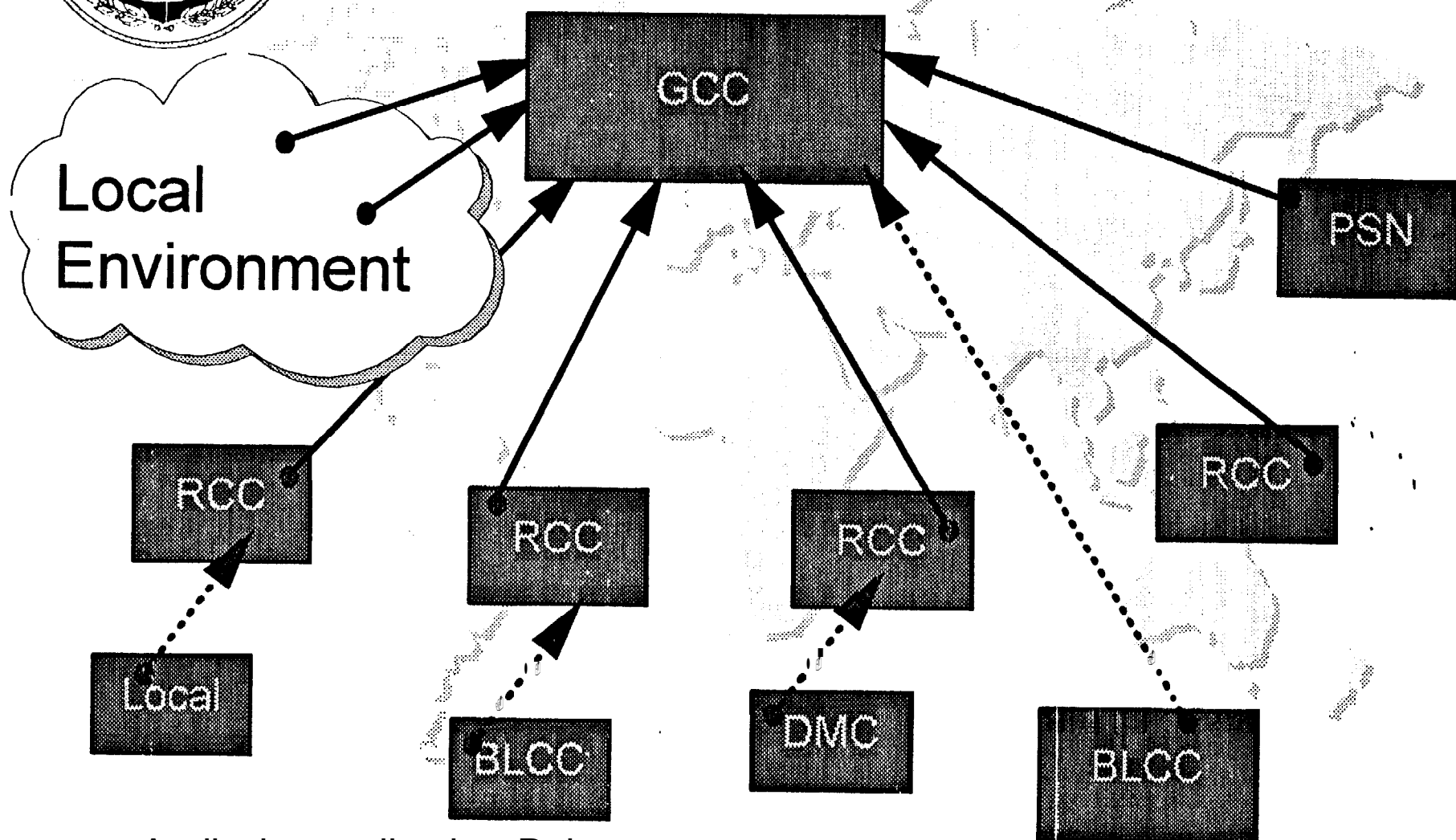
Global/Regional Control Center

A Functioning View





Hierarchal 'Relations

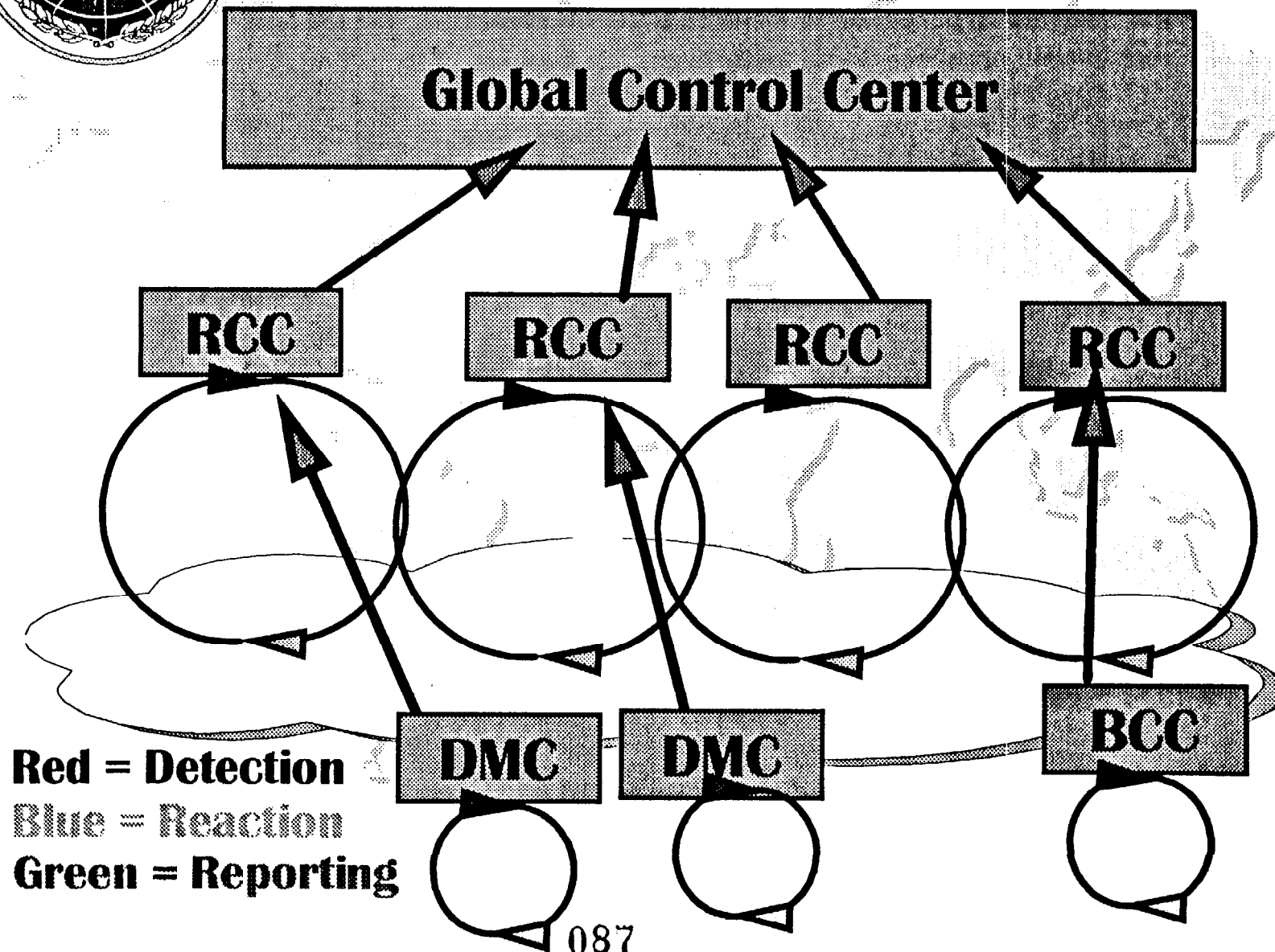


- Audit data collection Points



Operating Modes

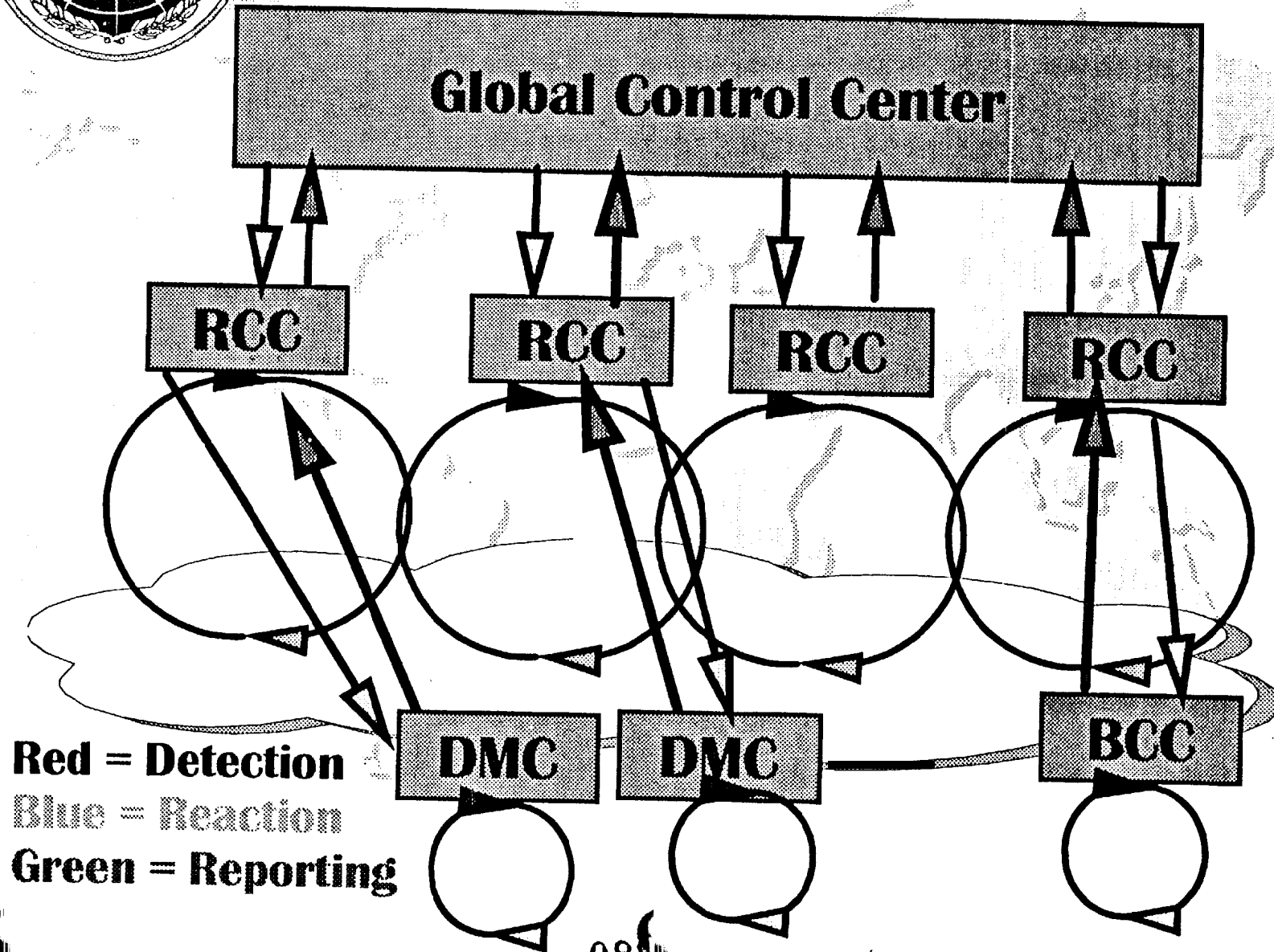
Routine Operations





Operating Modes

Crisis Operations





GCC/RCC Functions

Vulnerability Detection (Continual VAAP)

Attack Recognition (AMIDS)

Prioritized Responses (AIMS)

Customer Support (BBSs/Alerts/Tools)

CINC Support Team

IW-D Battlespace

Wargames and Exercises

Incident Response (DoD, National, International)



GCC/RCC Requirements

Audit Monitoring/Intrusion Detection (AMIDS)

Malicious Code Detection Eradication (h&DES),

Automated Infrastructure Management (AIMS)

Vulnerability Analysis (VAAP)

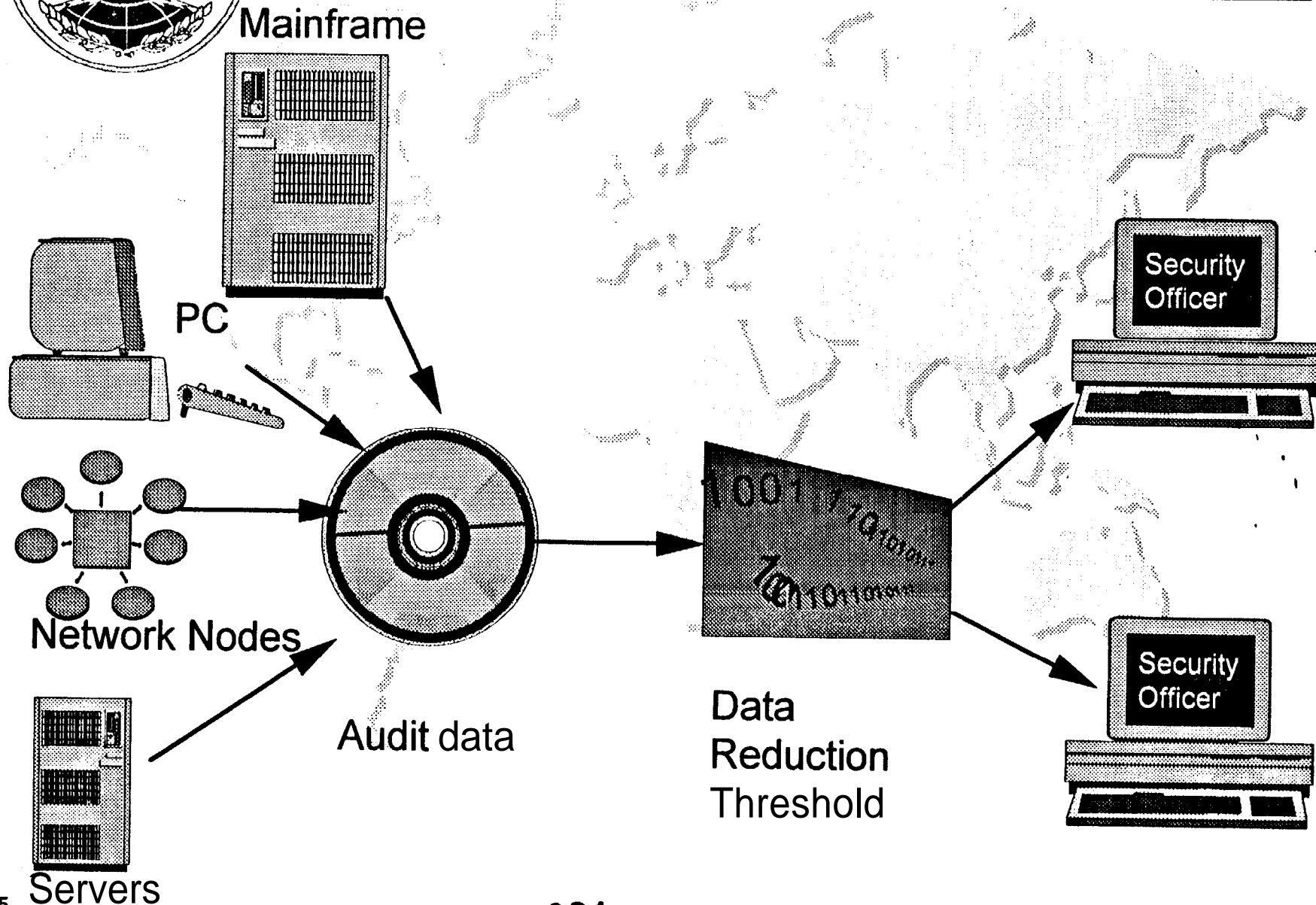
Personnel, Training, and Facilities

Wargames and Exercises

Reserve Components



Audit/Monitoring Intrusion Detection System





Audit Monitoring/ Intrusion Detection System

Detect unauthorized activity as it occurs

Examples

- Intrusions
- Password Attacks
- Increased Privilege
- Disabling of Audits
- Denial of Service

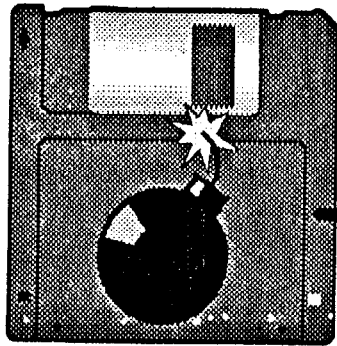
Task Number 5.5.1	FY96*	FY97	FY98	FY99	FY00	FY01
Identify, Evaluate, and Select COTS/GOTS AMIDS	△→△					
Acquire and Field Systems Hardware and Software		△				
Integrate and Standardize AMIDS Product Across Heterogeneous Operating Systems		△→△				
Expand Capabilities of Selected Products		△→△				
Maintain AMIDS						

* FY96 activities conducted with Government manpower and resources

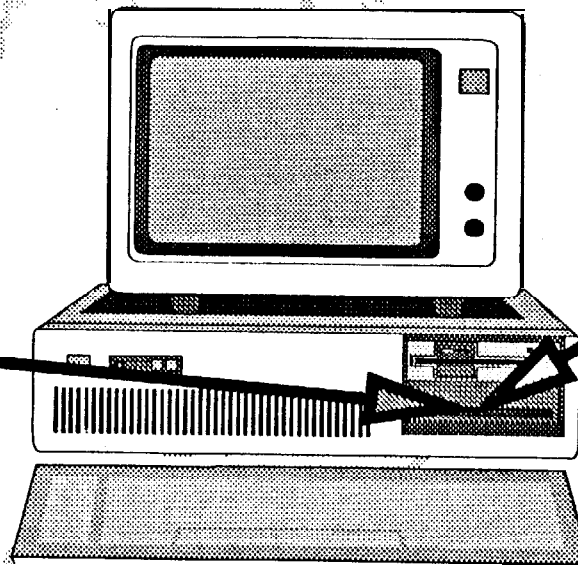


Malicious Code Detection/ Eradication System

Today

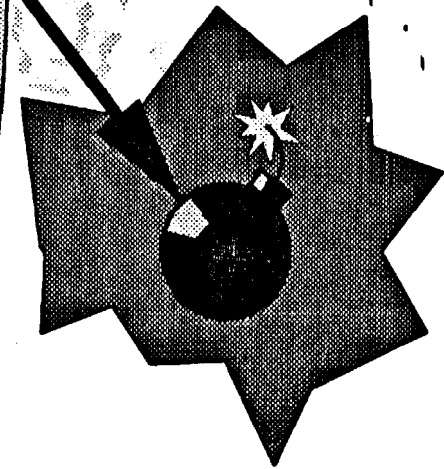
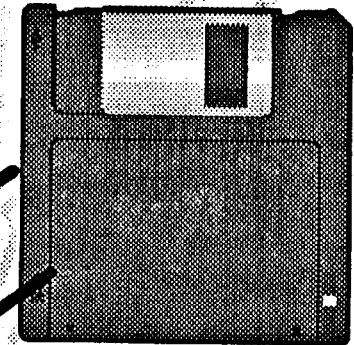


Virus introduced
into computer



Detects malicious
code before
introduction into DII
computer

Planned

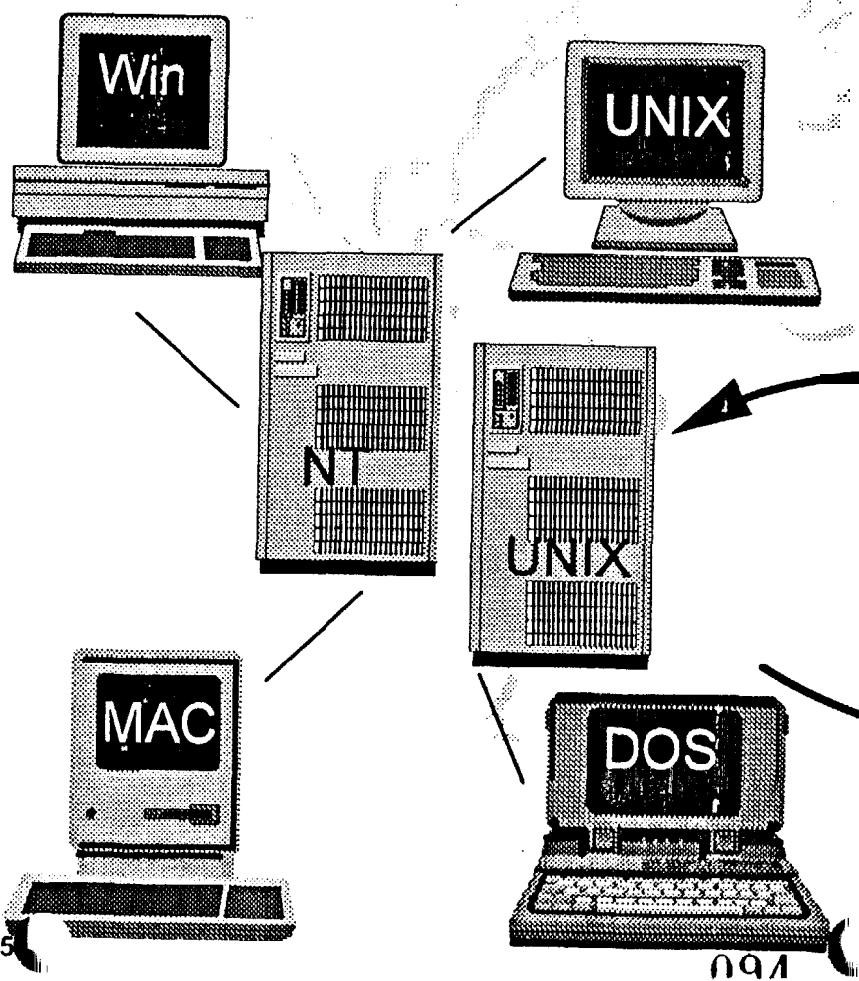




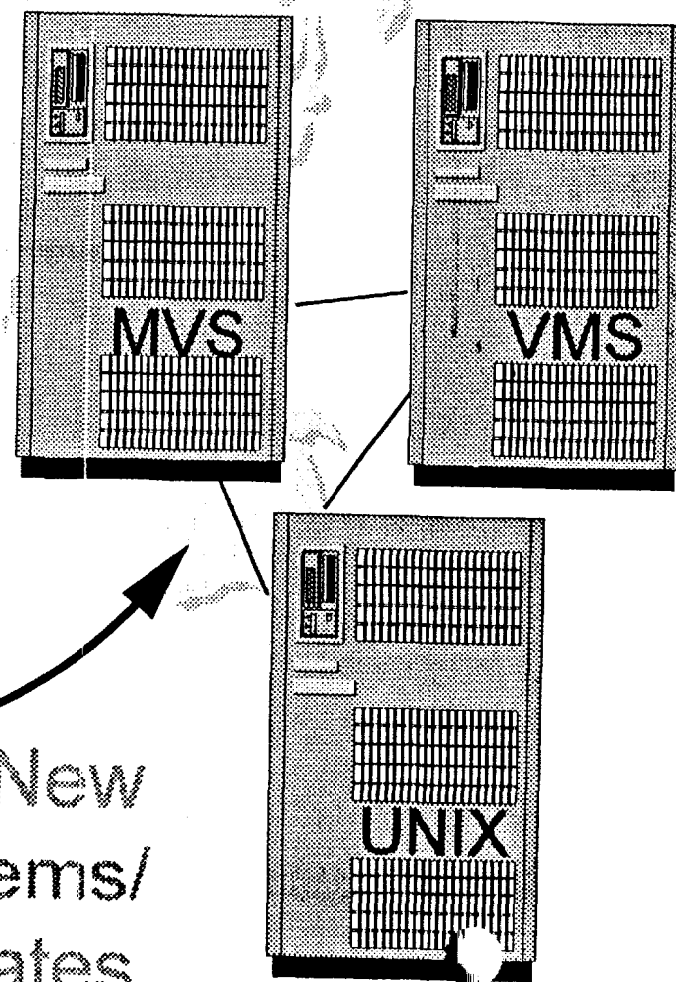
Malicious Code Detection Eradication

Normal Operations

Local Environment



Central System



Push
Updates

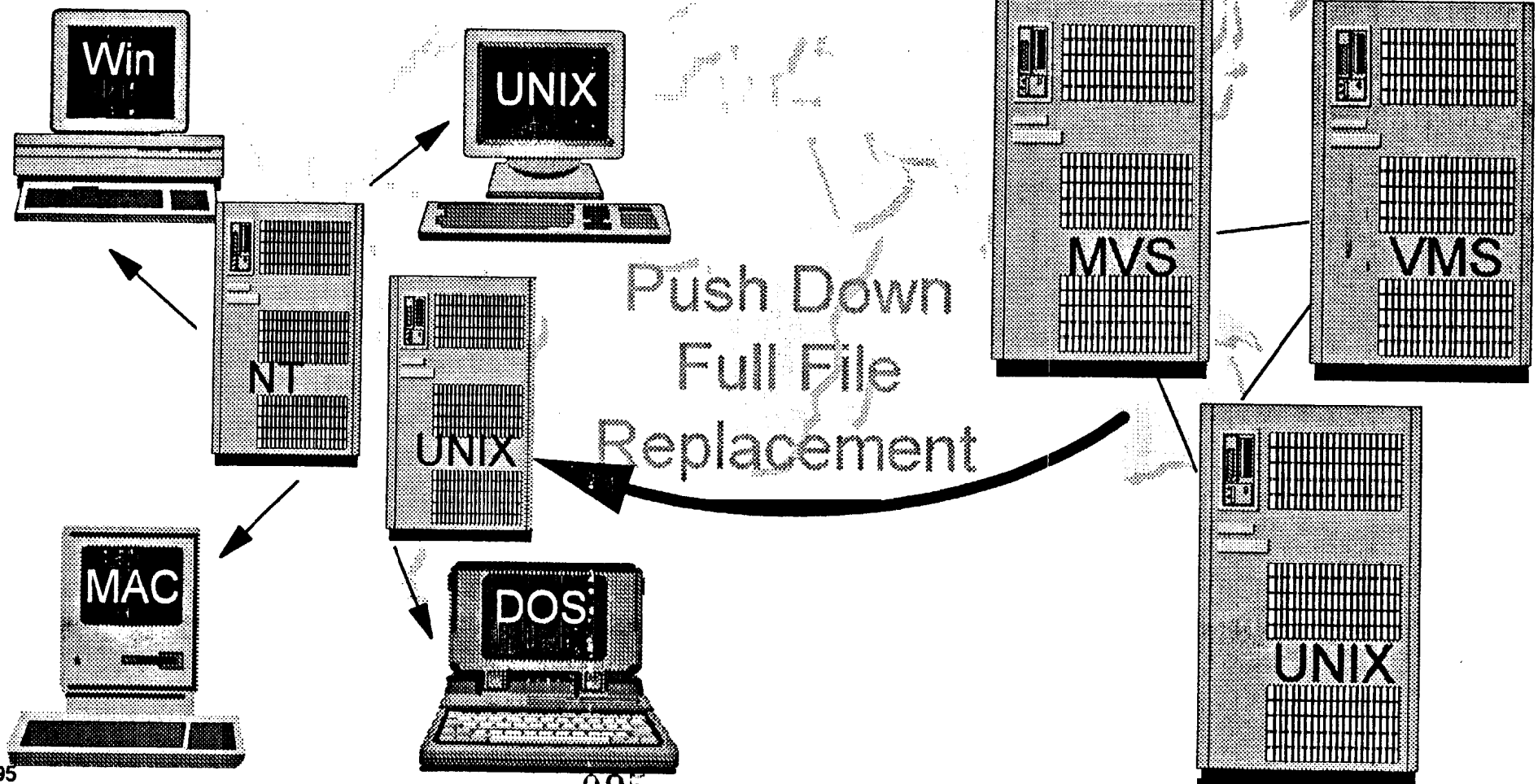
Pull New
Systems/
Updates



Malicious Code Detection Eradication Contingency Operations

Local Environment

Central System





Malicious Code Detection Eradication System

Detect Irregular Code Examples

- . Viruses
- Trojan Horses
- Time Bombs
- Spoofing Tools
- Sniffers

Task Number 5.5.2	FY96*	FY97	FY98	FY99	FY00	FY01
Develop Acquisition, Maintenance, and Distribution Concept	△→△					
Identify, Evaluate, and Select COTS/GOTS MCDES	△→△					
Acquire Hardware/Software for MCDES		△→△				
Modify and Enhance MCDES			△→△			
Maintain MCDES		△→△				

*FY96 activities conducted with Government manpower and resources



IW-D "REACT"

Example Responses

- Alternate Network Routing
- Prioritized Network Service Levels
- Move Service From Digital Networks To Satellite Systems
- Frequency Re-allocation
- Communications Isolation
- Response Team Dispatch
- Fall Back Processing
- NSEP Activation
- "Patch" Development and Deployment



Automated Infrastructure' Management

Manage and Control the DII Under Attack

Examples

- Terrestrial/Satellite
- Isolation
- Restoral
- Alternate Routing
- Fallback Processing

Task Number 5.5.4	FY96*	FY97	FY98	FY99	FY00	FY01
Investigate Existing Capabilities	△→△					
Select, Modify, and Integrate AIMS		△→△				
Field AIMS in GCC/RCCs		△→△				
Maintain and Enhance			△→△			

*FY96 activities conducted with Government manpower and resources



Vulnerability Analysis and Assessment Program

Detect Potential Problems in Systems

Targets

- Assessments
- Components
- Procedures
- Facilities
- Personnel

Task Number 5.4.2	FY96*	FY97	FY98	FY99	FY00	FY01
Conduct UNIX Systems Vulnerability Assessments	△					△
Conduct Mainframe Computing Systems Vulnerability Assessments		△				△
Conduct Networking Vulnerability Assessments			△			△
Conduct Telephony Vulnerability Assessments				△		△
Conduct Vulnerability Assessments on Other Systems (e.g., PCs, Environmental Controls)				△		△






Personnel and Training

Prepare People to Support GCC/RCC

Examples

- Info-warrior
- Retrain
- SCI Cleared
- 200 Security Personnel
- Reserve Components Utilization Plan

Task Number 5.5.5B	FY96	FY97	FY98	FY99	FY00	FY0 1
Retrain RCC Specialists						
Maintain the Facilities and Technical Proficiency Training Program						



Facilities

Prepare People & Facilities to Support GCC/RCC Examples

- SCIF is Required
- Backup Site
- Power (UPS)
- Equipment (AIS/Housekeeping)
- Communications (New/Redundant)








Task Number 5.5.5A	FY96	FY97	FY98	FY99	FY00	FY01
Prepare GCC and RCCs Facilities to Provide IW-D Detect and React	△	GCC △	RCC △	△		
Build Out Facility		GCC △	RCC △			
Incorporate GII View into the GCC and RCCs			△	△		



Wargames and Exercises

Practice and Test Plans Examples

- Red Team
- Prototype
- Implement
- Exercise

Task Number 1.5	FY96	FY97	FY98	FY99	FY00	FY01
Review Red Team Operational Concepts						
Develop Wargame and Exercise Concepts						
Develop and Test Prototype Wargames and Exercises						
Develop and Implement Wargames and Exercises						
Include Exercises in Joint Exercises						



Reserve Components

Augment with Experts Examples

- Peacetime Tests
- Contingency
- Expertise
- Practice

Task Number 1.6	FY96*	FY97	FY98	FY99	FY00	FY01
Develop CONOPS and Realign Reserve Utilization in DISA for IW-D/INFOSEC Support	△	△				
Provide Increased IW-D/INFOSEC Support to GCC/RCC/DMCs and MSTs in Peacetime, Exercise and Contingency Crisis Operations		△				

*FY96 activities conducted with Government manpower and resources



General Security Support

Examples

. Architecture and Engineering

- Standards
- Testing
- Tech. Insert.
- . Modeling & Sim.

Task Number 6.4	FY 96	FY 97	FY98	FY99	FY00	FY01
Frame the Problem		▲▲				
Develop Rapid Prototypes		▲▲				
Make Simple Modification to Existing Models		▲▲				
Develop and Integrate IW Modules with Existing C4I Simulations			▲	▲		
Prototype IW Modules for GCCS Training Environment			▲	▲		



INVESTMENT Program

Research and development to:

Maintain technological currency of existing security products

Develop new security products for digital networks:

- Replace analog secure (STU-III) with digital secure telephone (STE)
- ▶ Secure digital cellular (wireless) telephone capability
- ▶ Secure high-capacity, digital broadcast capability for tactical forces



Information Warfare

Response To A New Reality

- **Defense planning must reflect anticipated realities**
 - Battle damage assumed, operation under stress
 - Response procedures and recovery capacity built in
- **Priorities must be properly addressed:**
 - Infrastructure
 - Operations
- **Criticality of information must be understood**
 - Operational need/impact of loss - time critical
- **We must train for defensive information warfare**
 - Train information warriors
 - Hold wargames, readiness drills and exercises